САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 4

Санкт-Петербург
2017

http://spoisu.ru

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 4

Санкт-Петербург
2017

http://spoisu.ru

УДК (002:681):338.98

Р32

Региональная информатика и информационная безопасность.

Р32 Сборник трудов. Выпуск 4 / СПОИСУ. – СПб., 2017. – 533 с.

ISBN 978-5-906841-69-8

В 4-й выпуск периодического издания «Региональная информатика и информационная безопасность» включены материалы докладов участников юбилейной X Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России» и юбилейной XV Санкт-Петербургской международной конференции «Региональная информатика», проведенных при поддержке Правительства Санкт-Петербурга. Сборник охватывает широкий круг направлений: Государственная политика в сфере информатизации и информационной безопасности; Информационная безопасность телекоммуникационных сетей; Безопасность информационных технологий; Современные средства защиты информации; Правовые аспекты информатизации и информационной безопасности; Информационно-экономическая безопасность; Подготовка и переподготовка ИТ-специалистов; Информационные технологии на транспорте; Информационные технологии управления объектами морской техники и морской инфраструктуры; Информационные технологии в экологии; Информационная безопасность киберфизических систем; Молодежная научная школа: Безопасные информационные технологии; Молодежная научная школа: Информационные технологии и проблемы устойчивого развития.

Предназначен для широкого круга руководителей и специалистов органов государственной власти и местного самоуправления, промышленности, науки, образования, бизнеса, аспирантов и студентов высших учебных заведений Санкт-Петербурга и других регионов, специализирующихся в вопросах информатизации, связи, информационной безопасности и защиты информации.

УДК (002:681):338.98

Редакционная коллегия: *Б.Я. Советов, Р.М. Юсупов, В.В. Касаткин*
Компьютерная верстка: *А.С. Михайлова*
Дизайн: *Н.С. Михайлов*

Публикуется в авторской редакции

Подписано в печать 03.11.2017. Формат 60x84⅛. Бумага офсетная.
Печать – цифровая. Усл. печ. л. 61,96. Тираж 240 экз. Заказ № 9813
Отпечатано в ООО «Политехника-принт»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-906841-69-8

© Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления (СПОИСУ), 2017 г.
© Авторы, 2017 г.

ST. PETERSBURG INTERREGIONAL CONFERENCE
INFORMATION SECURITY OF RUSSIAN REGIONS

ST. PETERSBURG INTERNATONAL CONFERENCE
REGIONAL INFORMATICS

Proceedings

REGIONAL INFORMATICS AND INFORMATION SECURITY

The Issue No 4

St. Petersburg
2017

http://spoisu.ru

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В СФЕРЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 1082.00

ИНФОРМАТИЗАЦИЯ НАЛОГОВОЙ СФЕРЫ В МОДЕЛИ ИДЕАЛЬНОГО ГОРОДА

Еремичев Даниил Андреевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, ул. Большая Морская, 67
e-mail: daneremichev@gmail.com

Аннотация. Работа посвящена внедрению инноваций, в данном случае информатизации, в налоговой сфере на модели идеального города. Разработан комплекс инноваций, которые могут повысить эффективность работы налоговых служб, а также существенно улучшить качество услуг, предоставляемых налоговыми органами.

Ключевые слова: *информатизация; вычислительный центр; налоговые органы; нейронные сети; дата-центр; комплекс; наука о данных; компьютерное зрение.*

INFORMATIZATION OF THE TAX SPHERE IN THE MODEL OF THE IDEAL CITY

Eremichev Daniil
St. Petersburg State University of Aerospace Instrumentation
Russia, St. Petersburg, Bolshaya Morskaya str., 67
e-mail: daneremichev@gmail.com

Abstract. Thepaper is devoted to the introduction of innovations, in this case, informatization, in the tax sphere on the model of an ideal city. A set of innovations has been developed that can improve the efficiency of the tax services, as well as significantly improve the quality of services provided by tax authorities.

Keywords: *informatization; computer center; tax authorities; neural networks; data center; complex; data science; computer vision.*

С начала 2000-годов использование информационных технологий в налоговой сфере увеличилось с 0.1% до 15.4% в 2016 году. Однако их часть всё равно крайне мала, чтобы соответствовать времени, их доля должна увеличиться в 1,5-2 раза, по сравнению с 2016 годом. Однако в наше время без использования передовых достижений в сфере искусственного интеллекта обработка огромного количества данных крайне сложна.

Основные проблемы налоговой сферы:

1. Непрерывное увеличение налогового документооборота (около 20%-40% в год)
2. Усложнение и постоянное изменение процедур налогового законодательства (по оценке экспертов в год изменяется около 40% алгоритмов расчёта).
3. Огромные трудозатраты на обработку налоговых документов (только трудозатраты на ввод первичных документов от юридических лиц составляет тысяч чел.-день по оценкам от 25% до 30% времени работников налоговых органов тратится на ручной ввод данных налоговой отчётности)
4. Низкая энергоэффективность работы контролирующих органов: в течение года налоговые органы выполняют 500 тысяч выездных проверок, (каждая из которых требует около 10 специалистов на 20-30 дней, но эффективность около 50%).

Основной задачей внедрения инновационных технологий в налоговую сферу является информатизация всей структуры налоговых органов: создание основного вычислительного центра (ОВЦ), ЭВМ обладающего огромной вычислительной мощностью с использованием технологий, основанных на нейронных сетях, а в частности из разработок на основе data science, такой тандем позволит ускорить работу и уменьшить время затрачиваемое ОВЦ на обработку документации, постройка дата-центра с большим потенциальным объемом данных и доступным ОВЦ, необходимо также создание оптоволоконной сети, связывающей ОВЦ и дата-центр для достижения максимальной скорости передачи данных, создание наиболее защищенной сети между всеми офисами налоговой службы, ОВЦ и дата-центра, для защиты от кибер-атак, также планируется обеспечить каждого сотрудника налоговых органов, отправляющихся на вызовы, отдельным планшетным ПК, для доступа

к данным в дата-центре и сети ФНС. Сотрудники в офисах ФНС будут оборудоваться только персональным ПК, принтером и остальной необходимой орг. техникой. Все крупные вычисления будут производиться с помощью облачных технологий и вычислительной мощностью ОВЦ. Вся бумажная документация не будет выходить за стены таких офисов и будет немедленно конвертироваться в цифровой вид с помощью технологии компьютерного зрения, основанной на искусственном интеллекте, с помощью этой технологии сотрудник будет получать эту документацию не в виде изображения, а уже в текстовом формате, что будет экономить время на вводе данных непосредственно сотрудником. Также планируется создание личных кабинетов налогоплательщиков, это сможет повлиять на загруженность офисов ФНС. Так при сокращении загруженности офисов можно сократить штат сотрудников офисов, хотя потребуется провести качественное обучение имеющихся сотрудников в сфере IT. При этом можно создать колл-центр для обеспечения более качественных услуг в данной сфере.

Стоимость проведения данной реформы может потребовать большое количество ресурсов: для создание вычислительного центра требуется создание отдельного комплекса, который должен быть построен вблизи электростанции, для обеспечения большого количество электроэнергии, требуемой вычислительном центром. Также он должен быть оборудован современной системой пожаротушения, оборудованием (DRUPS), накапливающим электроэнергию, на случай отключения сети, что даст время для запуска генераторов, постройка этих самых генераторов, создание запаса топлива. Также такой большой комплекс будет вырабатывать огромной количество тепла, для предотвращения этого нужно построить оборудование для охлаждения комплекса, потребуется установка высокотехнологичного электрического оборудования для поддержания нормального функционирования электросети.

Инновации в налоговой сфере не должны заканчиваться только на улучшении оборудования также чтобы ввести налоговую службу в новое время, мы должны пересмотреть и законодательную часть:

Наиболее интересной идеей, основанной на использовании искусственного интеллекта, можно считать обучение нейронной сети для построения налоговых ставок, взяв за основу множество данных таких как: потребительская корзина, доход, платежеспособность, расходы. Поручив это машине, мы можем получить наиболее объективные данные.

Динамическая налоговая ставка применяется во многих развитых странах. Данная реформа позволит улучшить качество жизни людям с низким доходом, поскольку уменьшение их подоходного налога увеличит их покупательную способность и улучшит качество жизни.

Налоговая сфера является одним из основных способов пополнения бюджета государства, в нашем случае, города. Эта сфера не может оставаться без внедрения инноваций. Информатизация сферы и пересмотренная законодательная часть являются одними из основных способов модернизации налоговой службы.

СПИСОК ЛИТЕРАТУРЫ:

1. Компьютерное зрение // Википедия. URL: https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B5_%D0%B7%D1%80%D0%B5%D0%BD%D0%B8%D0%B5 (дата обращения: 26.11.2017).
2. Налоговая статистика // Петростат. URL: http://petrostat.gks.ru/wps/wcm/connect/rosstat_ts/petrostat/resources/5330fd804d2c57b8beefbef5661033e3/02nal_g.pdf (дата обращения: 26.11.2017).
3. Наука о данных // Википедия. URL: Компьютерное зрение // Википедия. URL: https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B5_%D0%B7%D1%80%D0%B5%D0%BD%D0%B8%D0%B5 (дата обращения: 26.11.2017). (дата обращения: 26.11.2017).

УДК: 004.78

ПРОБЛЕМЫ ПОСТРОЕНИЯ СИТУАЦИОННЫХ ЦЕНТРОВ СУБЪЕКТОВ ФЕДЕРАЦИИ В УСЛОВИЯХ ПЕРЕХОДА К ЦИФРОВОЙ ЭКОНОМИКЕ

Жигадло Валентин Эдуардович
Филиал ФГУП ЦНИИС – ЛО ЦНИИС
Россия, Санкт-Петербург, Варшавская ул., 11, лит. А
e-mail: zve@mail.ru

Аннотация. В современных условиях эффективность процесса управления жизнедеятельностью современных крупных городов и регионов определяется наличием высокоэффективных центров управления жизнедеятельностью мегаполисов. В статье подробно рассматриваются проблемы построения ситуационных центров субъектов федерации в условиях перехода к цифровой экономике, их роль и место в системе управления городским хозяйством, основанной на принципах «Умного Города».

Ключевые слова: *безопасный город; Умный Город; ситуационный центр; информационная система; система распределенных ситуационных центров.*

PROBLEMS OF CREATION OF THE SITUATIONAL CENTERS OF TERRITORIAL SUBJECTS OF THE FEDERATION IN THE CONDITIONS OF TRANSITION TO DIGITAL ECONOMY

Zhigadlo Valentin
1Branch of the Federal state unitary enterprise TSNIIS – LO TSNIIS
Russia, St. Petersburg, Varshavskaya St., 11, lit. A
e-mail: zve@mail.ru

Abstract. In modern conditions the efficiency of process of management of activity of the modern large cities and regions is defined by existence of highly effective control centers of activity of megalopolises. In article problems of creation of the situational centers of territorial subjects of the federation in the conditions of transition to digital economy, their role and the place in the control system of municipal economy based on the principles of "the Clever City" are in detail considered.

Keywords: *safe city; "Smart City"; situational center; information system; information system; system of the distributed situational centers.*

Современное развитие информационного общества характеризуется интенсивным внедрением на региональном уровне различных автоматизированных информационных систем (АИС), направленных на повышение эффективности управления различными сферами, как экономики, так и городского хозяйства, а также городского (территориального) управления. Особое место среди задач информатизации в последний период стала занимать задача создания информационных систем сбора, накопления, анализа информации и поддержки принятия управленческих решений в области безопасности жизнедеятельности крупных мегаполисов, промышленных территорий и особо опасных объектов.

Примерами таких систем служат - АПК (АИС) «Безопасный город», Комплексная система обеспечения безопасности жизнедеятельности как муниципального, так и регионального уровней (КСОБЖН), АИС ЦУКС МЧС, Система «Умный Город» (рис.1). В основном данные системы создавались эволюционно в разные периоды времени и имеют различную ведомственную подчинённость при совпадении целей и задач:

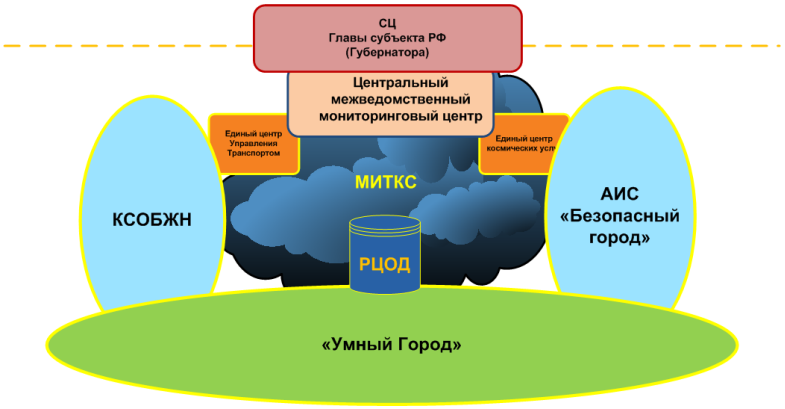


Рис. 1. АИС Субъектов Федерации

1. Аппаратно-программный комплекс «Безопасный город» – носит ведомственную принадлежность МВД и МЧС. АПК «Безопасный город» предназначен для повышения уровня общественной безопасности и безопасности среды обитания за счет создания комплексной информационной системы, обеспечивающей прогнозирование, мониторинг и предупреждение возможных угроз, а также контроль устранения последствий чрезвычайных ситуаций и правонарушений с интеграцией под ее управлением действий информационно-управляющих подсистем различных организаций (дежурных, диспетчерских, муниципальных служб) с обеспечением их оперативного взаимодействия в интересах муниципального образования. Сегменты АПК «Безопасный город» представлены на рис. 2 [3].

Основными задачами построения и развития АПК «Безопасный город» являются [3]:

– формирование информационно-коммуникационной платформы для органов местного самоуправления с целью устранения рисков обеспечения безопасности среды обитания, общественной безопасности и правопорядка на базе межведомственного взаимодействия;

– разработка единых функциональных и технических требований к аппаратно-программным средствам, ориентированным на идентификацию потенциальных точек уязвимости, прогнозирование, реагирование и предупреждение угроз обеспечения безопасности муниципального образования;

– обеспечение информационного обмена на федеральном, региональном и муниципальном уровне через единое информационное пространство с учетом разграничения прав доступа к информации разного характера;

– создание дополнительных инструментов (АИС) на базе муниципальных образований для оптимизации работы существующей системы мониторинга состояния общественной безопасности;

– построение и развитие систем ситуационного анализа причин дестабилизации обстановки и прогнозирования существующих и потенциальных угроз для обеспечения безопасности населения муниципального образования.

Рис. 2. **Сегменты** АПК «Безопасный город»

Базовым элементом безопасного города является комплекс средств автоматизации "Единый центр оперативного реагирования" (КСА ЕЦОР). КСА ЕЦОР – это объединение программно-аппаратных средств для комплексной информатизации процессов Единой дежурно-диспетчерской службы (ЕДДС). Комплекс повышает уровень безопасности, комфорта проживания и эффективности управления городом.

Центр Управления Кризисными Ситуациями (ЦУКС) – предназначен для решения задач прогноза возникновения и ликвидации последствий ЧС, носит ведомственную принадлежность МЧС.

2. Основными задачами ЦУКС являются [4]:

– реализация единой государственной политики в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуации, обеспечения пожарной безопасности на территории соответствующего региона Российской Федерации;

– обеспечение боевой и мобилизационной готовности (готовности к применению) органов, специально уполномоченных решать задачи гражданской обороны, задачи по предупреждению и ликвидации чрезвычайных ситуаций, в составе или при органах исполнительной власти субъектов Российской федерации и органах местного самоуправления (далее — орган управления по делам гражданской обороны и чрезвычайным ситуациям), спасательные воинские формирования, органов управления и подразделений Государственной противопожарной службы, организаций и поисково-спасательных формирований МЧС России, дислоцированных на территории соответствующего региона Российской Федерации;

– осуществление в установленном порядке мер по организации и ведению гражданской обороны, защите населения и территорий от чрезвычайных ситуаций и пожаров, а также мер по чрезвычайному гуманитарному реагированию на территории соответствующего региона Российской федерации;

– осуществление координации функционирования территориальных подсистем единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (далее — РСЧС);

– осуществление в установленном порядке сбора, обработки и обмена информацией в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности;

– управление в пределах своих полномочий соединениями, воинскими частями и организациями войск гражданской обороны, подразделениями Государственной противопожарной службы, а также поисково-спасательными формированиями поисково-спасательной службы МЧС России, дислоцированными на территории соответствующего региона Российской Федерации.

3. КСОБЖН – направлена на обеспечение безопасности жизнедеятельности населения Субъекта федерации, муниципального образования.

Комплексная система обеспечения безопасности жизнедеятельности населения — это совокупность организационных структур в сфере государственного управления, взаимосвязанных подсистем мониторинга и прогнозирования ЧС природного, техногенного и иного характера, контроля состояния потенциально опасных и других объектов защиты, объединенных в целях информационной поддержки принятия решений о предупреждении и ликвидации ЧС, оповещения и информирования населения о действиях при угрозе ЧС и в условиях ЧС, управления силами ликвидации ЧС (рис. 3).

КСОБЖН создаются в регионах начиная с 2009 года, в соответствии с Концепцией, утвержденной МЧСРоссии, МВД России и ФСБ России и реализуются в рамках федеральной целевой программы или иной программы соответствующего уровня и финансирования, в том числе за счет средств бюджетов субъектов Российской Федерации, органов местного самоуправления и организаций.

«Умный город» - предназначен для решения задач управление всеми аспектами жизни региона и городского хозяйства - Субъекты федерации.

Умный город – это комплекс организационных мероприятий и программно-технических решений, направленных на устойчивое социально-экономическое развитие города, создание высокотехнологичной наукоемкой экономики, эффективное использование всех видов ресурсов (электричество, вода, газ/тепло, пространство, время) и создающих условия для удобного и безопасного пребывания в городе, комфортного проживания и ведения бизнеса (рис. 4).

Предлагаемые и реализуемые за рубежом и в России стратегии, концепции, подходы, модели и проекты по созданию Умных городов, можно свести к общей модели, включающей семь составляющих: умная экономика; энергоэффективность и ресурсосбережение; умная среда обитания; мобильность; умное население; умное управление; комфортность проживания.

«Умный Город» для городских властей [5] – это: обеспечение мер безопасности и эффективное управление деятельностью экстренных и оперативных служб; мониторинг и управление угрозами и чрезвычайными ситуациями, влияющими на среду обитания; переработка и утилизация отходов производства и потребления (мусора), раздельный сбор мусора; очистка сточных вод, управление ливневыми стоками; энергоэффективность и ресурсосбережение (использование энергосберегающих, экологичных и безопасных технологий и решений в топливно-энергетическом комплексе (включая водоснабжение), ЖКХ, градостроительстве и на транспорте); комфортное жильё, умный дом/здание; система городского оперативного оповещения; многофункциональные центры (МФЦ), обслуживающие жителей и организации по принципу «одного окна», государственные и муниципальные услуги, а также дополнительные информационные, заказывающие и платежные сервисы в электронном виде в сфере ЖКХ, связи, транспорта, торговли, быта, банковского обслуживания, налогов, страхования, культуры, спорта, отдыха, туризма и пр; городское видеонаблюдение для предотвращения правонарушений; система фиксации нарушений ПДД и сбора штрафов; планирование расходов на оплату коммунальных услуг бюджетных организаций; удобный общественный транспорт, транспортная доступность, снижение загруженности УДС, отслеживание «пробок» и управление дорожным движением; градостроительство и землепользование в соответствии с принципами архитектуры нового урбанизма и промышленной архитектуры индустриальных парков и их совместимости; экологический и биологический мониторинг окружающей среды (атмосфера, гидросфера, почва, биосфера), использование возобновляемых источников энергии (солнечные, ветряные, геотермальные, приливные, биотопливные); GPS/GLONASS мониторинг городского транспорта и транспорта экстренных служб; обслуживание общегородской инфраструктуры; прозрачное предоставление образовательных услуг (электронное образование); прозрачное предоставление медицинских услуг (электронная и телемедицина); информационно-картографическое обеспечение и т.п.

«Умный Город» для жителей - это: система самообслуживания через личный кабинет для оплаты услуг ЖКХ, электронная запись для получения бытовых или медицинских услуг; решения по экономному расходованию всех видов коммунальных ресурсов; быстрое предоставление государственных услуг городскими властями; карта жителя города (ID, проезд в городском транспорте, система предоставления скидок, оплата за товары и услуги); внутридомовое (входы в здания, лифты, этажные площадки...) и наружное видеонаблюдение, системы видеоконференцсвязи (ВКС) и телеприсутствия; интеллектуальная транспортная система, парковочный информатор, электронное расписание (графики работы и обслуживания, транспорт); системы погодно-климатического и экологического мониторинга; градостроительство и землепользование в соответствии с принципами архитектуры нового урбанизма (пешеходная доступность в частности); скоростная ИКТ-инфраструктура (проводная и беспроводная), публичные и социальные сервисы на базе открытых интернет-порталов (Web-приложений) и мобильных приложений; высокотехнологичные многофункциональные персональные ИКТ-устройства, мобильные, информационные и платежные сервисы, электронные пластиковые карты (ID, различные виды платежей, безопасность, банковские, транспортные и др. виды услуг).

«Умный Город» для управляющих и ресурсо-снабжающих компаний - это: система автоматизированного сбора данных с приборов учета и мониторинга оборудования инженерных

систем, находящихся на обслуживании; система автоматизированного управления инженерными системами, погодно-ориентированное поведение инженерных систем; своевременное выставление счетов и контроль оплат, планирование расходов на оплату коммунальных услуг бюджетных организаций; решения по экономному расходованию всех видов коммунальных ресурсов; отчеты в режиме реального времени по потреблению всех видов ресурсов, как в масштабе города, так и в более мелкой детализации (квартал, здание, квартира, организация и т.п.); краткосрочные и долгосрочные прогнозы по потреблению ресурсов; видео-мониторинг за подотчётной территорией; обеспечение автоматического и диспетчерского отключения систем при наступлении природных или техногенных катастроф.

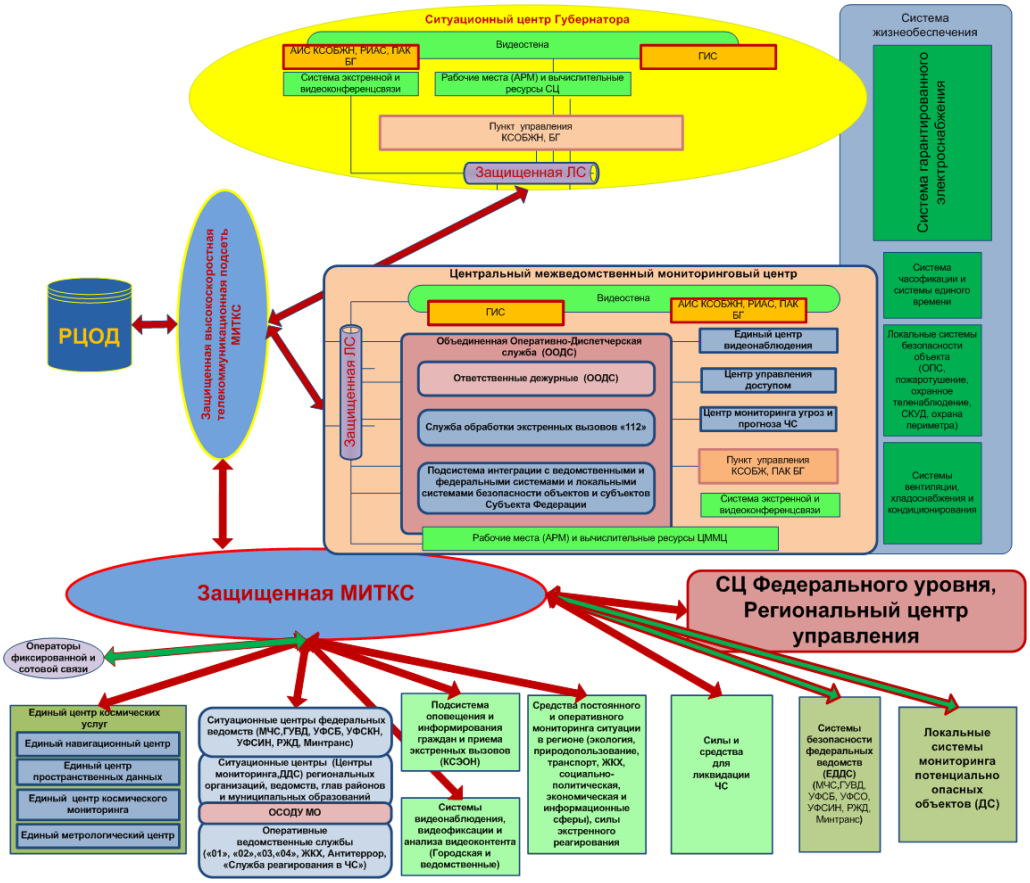


Рис. 3. Структура КСОБЖН

Рис. 4. Решение «Умный Город»

Согласно программе «Цифровая экономика», в России планируется к 2025 году создать 50 «Умных городов», в 2018 г. должна быть готова соответствующая концепция, а к 2025 г. - разработана модель деятельности «Умного» города с описаниями его объектов и отношений между ними. В 2025 г. в 50 городах будет внедрена интегрированная цифровая платформа управления, с помощью которой будет принимать 75% решений об управлении городскими ресурсами. Численность населения городов, участвующих в реализации концепции «50 «Умных городов России» должна составить, к 2020 году – 25 миллионов человек, к 2025 году – 50 миллионов человек.

Приказом Федерального агентства по техническому регулированию и метрологии № 642 от 27 марта 2017 года сформирован технический комитет по стандартизации 194 «Киберфизические системы» (ТК-194). К его задачам относится стандартизация «Умного города» (Smart City), «Интернета вещей» (Internet of things), «Больших данных» (Big data) и «Умного производства» (Smart manufacturing).

Основные противоречия, сложившиеся при создании вышеперечисленных систем:

1) Различная ведомственная принадлежность при совпадении целей и задач:

– БГ – безопасность дорожного движения, безопасность жизнедеятельности и правопорядок (носит ведомственную принадлежность МВД и МЧС);

– ЦУКС – прогноз возникновения и ликвидация последствий ЧС (носит ведомственную принадлежность МЧС);

– КСОБЖН – безопасность жизнедеятельности населения – (создается органами государственной власти Субъектов Федерации, МО);

– «Умный город» - управление всеми аспектами жизни региона и городского хозяйства (создается органами государственной власти Субъектов Федерации).

2) Использование системами, с различной ведомственной принадлежностью, одних и тех же элементов инфраструктурных систем (СЦ, Мониторинговый центр, Защищенная телекоммуникационная сеть, ЦУТ, ЦОД), создаваемых и принадлежащих, как правило, Субъекту федерации.

3) Системы БГ, КСОБЖН являются, по сути, элементами системы «Умный город» и должны входить в его состав как полнофункциональный элемент, а не как сопрягаемая ведомственная подсистема, соответственно, нужна единая межведомственная программа создания систем «Умный город», или, по крайней мере, единая концепция. Однако если ее разработку опять поручат какому-либо министерству, то идея интегральной, региональной системы, создаваемой в интересах региона (губернатора) будет потеряна.

В настоящее время, в условиях нарастания внешних и внутренних угроз устойчивому социально-экономическому развитию Российской Федерации, возрастает актуальность скорейшего создания и использования единой системы распределенных СЦ (СРСЦ) [1], интегрирующейся с созданной в РФ системой центров управления обороной РФ, направленной на решение задач поддержания Вооружённых сил Российской Федерации в боеспособном состоянии, а также для выполнения других информационных и координационных задач по обеспечению национальной безопасности Российской Федерации, и предназначенной для информационно-аналитической поддержки государственного управления и стратегического планирования (рис. 5).

Возрастающая динамика поступления новой информации обуславливает необходимость принятия незамедлительных управленческих решений, что особенно актуально при кризисных ситуациях в экономике или при чрезвычайных ситуациях природного или техногенного характера.

Ситуационные центры (СЦ) призваны помочь руководителям из различных отраслей экономики или сфер государственного управления комплексно и оперативно решать возникающие управленческие задач. СЦ создаются в органах государственной власти, в том числе в области обеспечения безопасности, а также на предприятиях военно-промышленного и топливно-энергетического комплексов. На настоящем этапе развития СЦ в органах государственного управления определяющими факторами являются создание и совершенствование системы взаимосвязанных СЦ всех уровней государственной власти, включая муниципальные образования, а также интеграция в единую систему ведомственных и корпоративных СЦ. Наибольшую актуальность представляет объединение созданных СЦ в единое информационное поле и организация межведомственного взаимодействия образования, управления природными ресурсами, экономикой и др.

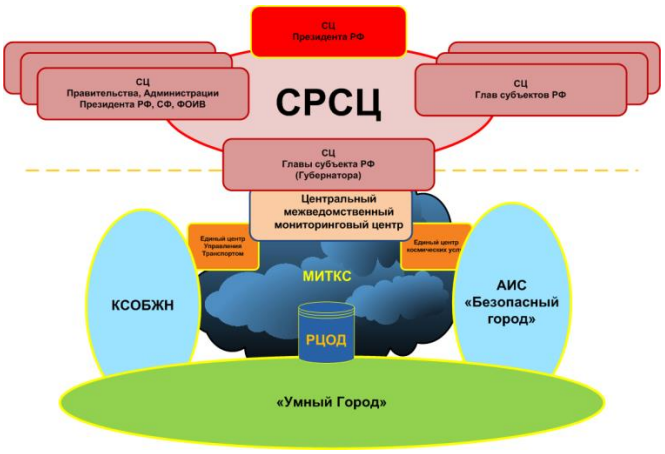


Рис. 5. Интеграция решений СЦРЦ на региональном уровне

Единая распределенная система СРСЦ призвана кардинально повысить эффективность информационно-аналитической поддержки реализации госполитики в сфере социально-экономического и общественного политического развития страны и обеспечения национальной безопасности, в том числе в условиях военного времени и при возникновении чрезвычайных (кризисных) ситуаций.

Однако, учитывая тот факт, что в регионах, крупных мегаполисах уже длительное время существуют и создаются СЦ, системы КСОБЖН, БГ, «Умный город», создание новой системы распределенных СЦ порождает ряд проблем, требующих своего незамедлительного решения.

Технические проблемы создания СРСЦ:

1) На региональном уровне при построении различных АИС (АПК БГ, КСОБЖН, АИС ЦУОК) существует ведомственная разобщенность и дублирование, как аппаратных платформ, так и программных сервисов для каждого информационного контура:

2) Функциональным элементом СРСЦ является ИАС, для реализации которой требуется выделенный и достаточно мощный вычислительный ресурс и ресурс СХД, но в структуре СРСЦ он не предусмотрен. При этом отсутствует четкая межведомственная программа по созданию в рамках СРСЦ единой распределенной структуры вычислительных ресурсов и СХД (ЦОД СРСЦ). По умолчанию, предполагается использование ЦОД, создаваемых субъектами федерации в регионах, но при этом отсутствуют единые требования по их построению (региональные ЦОД существенно отличаются между собой вычислительной мощностью, мощностью СХД, принципами структурного построения).

3) Отсутствует координация деятельности федеральных и региональных СЦ на основе единых информационного и административного регламентов, единых регламентов взаимодействия, единых форматов и протоколов.

4) Существующие АИС и СЦ губернатора охватывает широкий спектр областей деятельности: экономику, социальныевопросы, управление региональными (или муниципальными) программами, геоинформационный анализ, которые выходят далеко за рамки перечня задач ИАС СРСЦ, но крайне необходимы для ее функционирования. В этой связи целесообразно в качестве информационно-вычислительного ресурса для реализации региональных компонент ИАС СРСЦ использовать ресурс имеющихся или создаваемых региональных ЦОД. Ситуационный центр не должен превращаться в средство проведения селекторного совещания на базе видео-конференц-связи.

Проблемы ИАС СРСЦ:

– Не сформирован типовой набор моделей, алгоритмов, методов решения задач многофакторного анализа, прогнозирования, текущего планирования (отраслевого и территориального), стратегического планирования, управления на федеральном и региональном уровнях.

– Информационные системы в федеральных и региональных органах государственной власти, предназначенные для обеспечения поддержки принятия решений, в части модельного аппарата носят локальный характер, не синхронизированы, имеют разные структуры информации, поэтому усложняют, а в ряде случаев, исключают возможность их комплексирования.

– Отсутствуют унифицированные модели, которые можно было бы проецировать на регионы и дорабатывать с учетом специфики субъекта Российской Федерации. Целесообразно составить при участии научных учреждений фонд моделей, которые позволяли бы регионам решать типовые задачи.

– Решение однотипных информационных задач в различных системах осуществляется с использованием различного, не унифицированного модельного аппарата, отсутствует единый для всех регионов регламент их построения, что затрудняет, а зачастую делает невозможной их интеграцию в рамках создаваемой ИАС СРСЦ.

Нормативно - правовые проблемы:

– Отсутствуют решения о порядке координации работ по созданию СРСЦ с другими крупными проектами (НЦУО РФ, интегрированная сеть связи для нужд обороны страны, безопасности государства и обеспечения правопорядка, ПАК «Безопасный город», КСОБЖН, Система «Умный город» и др.).

– Отсутствуют системотехнические решения по построению СРСЦ, в том числе решения по защите информации. Программа создания СРСЦ должна предусматривать комплекс работ по созданию системообразующих компонентов, вводу в действие СЦ и поддержанию их функционирования.

СПИСОК ЛИТЕРАТУРЫ

1. Резолюция 4-й конференции «Система распределенных ситуационных центров − 2014», 16−17 октября, г. Воронеж.
2. Резолюция 5-й конференции «Система распределенных ситуационных центров», 7-9 октября 2015 г., г. Ярославль.
3. Концепция построения и развития аппаратно-программного комплекса «Безопасный город», утвержденная распоряжением Правительства Российской Федерации №2446-р от 03 декабря 2014 года;
4. Наставление по организации деятельности центров управления в кризисных ситуациях МЧС России, Москва, 2012 г.
5. В. Чернышев. Инфраструктура «Умного Города» - оптимальные решения, CNews Conferences, Москва, 2013 г.

УДК 1082.00

ПРОБЛЕМЫ УМНОГО ГОРОДА

Зыкова Галина Сергеевна, Артамонов Леонид Эдуардович, Елизов Валентин Олегович
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, Большая Морская ул., 67
e-mail: linazykova18@gmail.com

Аннотация. Рассмотрена концепция умного города. Также представлены наработки и инновации, придуманные студентами СПбГУАП.

Ключевые слова: *умный город; машиностроение; умный дом; будущее; инновации; моделирование; автомобильный кластер.*

THE PROBLEMS OF SMART CITY

Zykova Galina, Artamonov Leonid, Elezov Valentine
The St. PetersburgStateUniversityofAerospaceInstrumentation
Russia, St. Petersburg, Bolshaya Morskaya str., 67
e-mail: linazykova18@gmail.com

Abstract. The paper presents the concept of Smart City and the developments and innovations invented by the students of SUAI.

Keywords: *smart city; innovation; modeling; smart home; future; medicine.*

На заседании рабочей группыпо IT-технологиям и конвергентным системам при губернаторе Санкт-Петербурга Георгий Полтавченко сделал очень важное заявление: «Наша задача – вооружить современного петербуржца всеми самыми последними достижениями научно-технического прогресса в преддверие технологического скачка, который нас ожидает в обозримом будущем. Многие отдельные элементы системы «Умный город» в Санкт-Петербурге уже внедрены или внедряются. Необходимо объединить эти наработки, и в дальнейшем централизовано развивать систему управления городской средой».

Таким образом, губернатор поддержал проект «Умный город Санкт-Петербург», который предполагает внедрение единой системы стратегического и оперативного контроля различных сфер жизнедеятельности с использованием самых современных информационных технологий.

Но вместе с процессом выполнения этой задачи возникают некоторые трудности и проблемы. Чтобы их избежать наша команда из 60-ти студентов первого курса моделирует свой «Умный город», который затрагивает все сферы нашей жизни: транспорт, медицина, образование, культура.

Студентам предлагается выбрать для разработки и анализа одну из подсистем города, изучить ее и придумать свое решение проблем, связанных с данной отраслью. При моделировании города как сложной системы город разделяется на более мелкие подсистемы, создается иерархическая система для управления проектом и студенческий коллектив осуществляет разработку всех подсистем и их интеграцию в единое целое.

Мы являемся руководителями нашего «Умного города», распределяем бюджет между отраслями, делегируем задачи студентов, а также обобщаем все идеи, которые предлагают наши коллеги. На протяжении семестра студенты придумывают новые идеи и решения, а также внедряют инновации в свои подсистемы. Итогом этой работы являются реферат каждого из студентов по выбранной теме. Так, например, студент Подрезов Данила, который разрабатывает подсистему «Авиастроение», предлагает полноценный автопилот для гражданской авиации. Это позволит увеличить безопасность перелетов и уменьшить цены на авиабилеты. Автопилот будет самообучаемый благодаря нейронным сетям. На первых этапах необходимо внедрять программный софт в самолеты с пилотами для обучения нейронных сетей, а в дальнейшем тестировать на симуляторах и небольших воздушных судах. На последних этапах будет происходить тестирование на полноценных самолетах для точных настроек автопилота. Со временем нейросеть полноценно заменит пилотов. С учетом тенденции роста технологий - это вполне осуществимо к 2025 году.

В свою очередь Троценко Юлия, которая представляет банковскую подсистему, вводит технологию «бескартных» бесконтактных оплат покупок, основанную на использовании аналогичной технологии, как в бесконтактных банковских картах. Необходимо создать маленький чип, который будет крепиться к верхней части уха человека. Чип с антенной (RFID-метка), передающий информацию о платеже по радиоканалу будет незаметен на верхней задней части уха, что обеспечит безопасность и вряд ли кто-то будет красть у вас что-то прямо с уха. В чипе должна быть система контроля покупки, то есть разрешения ее совершения, оплаты товаров. Работать это должно следующим образом: человек подходит к кассе, ему пробивают все товары, а затем он, допустим, посредством определенной кнопки на чипе или жеста, или голосового сигнала разрешает терминалу списание средств с устройства. Таким образом, экономиться время и облегчается сам процесс покупки товаров.

Поляков Дмитрий рассмотрел концепцию «умного автомобиля». Разработка нового автомобиля, оснащенного новейшими технологиями и информационно-вычислительными системами, способными помочь водителю ориентироваться в сложной городской среде – основная задача создателей автомобилей. Для качественной работы «умного автомобиля» требуется сложная вычислительная система с большим количеством датчиков, приборов, сенсоров, исполнительных устройств и управляющих блоков. Автомобиль, включающий в себя все вышеперечисленные функции и технологии, будет соответствовать концепции «умного города», так как все они направлены на обеспечение безопасности водителя и пешеходов, а также экологию города. Применение данных систем приведет к минимуму количество ДТП, снизит информационную нагрузку водителя, улучшит видимость водителю, уменьшит загрязнение окружающей среды.

Родион Колесник поставил перед собой задачи рассмотрения и внедрения новых и инновационных идей в российскую систему здравоохранения. Основная инновация – это создание персональных электронных карт. Идея заключается в том, что многие люди сейчас используют различные приложения для смартфонов для создания графика спортивных занятий. Эти приложения используют биологическую информацию: пульс, давление, изменение веса. Так же существуют приложения, позволяющие человеку нормализовать свой сон. Мониторинг состояния человека сможет на ранних стадиях предотвратить различные болезни.

Новосвит Андрей предлагает свои инновации в области «Компьютеростроения». Например, голограммный монитор в пространстве (x, y, z), который работает точно также, как и монитор, но с помощью гаптоклона возможно перемещение картинки в пространстве (x, y, z). Благодаря этому пользователь может манипулировать голограммой так, как ему будет нужно. Голограммный экран можно увеличивать в любом масштабе, менять яркость и красочность. Клавиатура с динамически меняющимися клавишами – это клавиатуре, к кнопкам которой можно назначать любые функции. Изображение и подписи на клавишах устройства меняются динамически, в зависимости от используемого приложения, или текущей раскладки.

Клестова Маргарита продумала концепцию «умного дома». Система «умный дом», обеспечивающая ресурсосбережение, комфорт и безопасность для всех жильцов, сама по себе не нова для рынка. Однако раньше позволить себе её могли лишь привилегированные единицы. Теперь эту систему можно использовать для многоэтажных домов. В основе современной концепции «умного дома» лежит идея объединения множества электронных устройств в один механизм, слаженно работающий на благо жильцов. Например, при резком изменении температуры воздуха, задымленности, несанкционированном проникновении внутрь и любых других внештатных ситуациях «умный дом» самостоятельно вызовет необходимую экстренную службу, а при наличии соответствующих технологических приспособлений сам начнёт тушение пожара и даже перекроет лопнувшие водопроводные трубы.

Внедрение интеллектуальной энергетикикурирует Коба Виктор. Речь идёт о развитии интеллектуальной энергетики, более известной в мире как smart-grid. Суть энергетической системы, построенной на принципах smart-grid, состоит в том, что она передает не только энергию, но и информацию. В этом случае потребитель, помимо энергии, получает ряд возможностей по взаимодействию с энергосистемой. Например, он может более гибко выбирать тарифы, планировать свое энергопотребление или выступать в роли поставщика электроэнергии (при соблюдении ряда условий он сможет сам продавать энергию, вырабатываемую его личными источниками энергии: ветряки, солнечные батареи, накопители и т.д.) и, как следствие, снижать затраты на электроэнергию.

Великосельцева Саша, отвечающая за подсистему торговли, предлагает создать магазины «Без касс». Идея заключается в создании приложения для онлайн-магазинов. Турникеты будут сканировать QR-код при входе в магазин, а камеры - распознавать покупателей. При покупке товара, он автоматически будет заносится в виртуальную корзину. Оплата будет производиться с прикрепленного к аккаунту покупателя счета.

Жабченко Анастасия хочет создать электронный паспорт. На основе единой компьютерной модели организма создаётся модель организма каждого пациента, компьютер производит анализ состояния каждого больного и выявляет максимально правильное лечение. Таким образом, предложенные системы вполне могут использоваться для контроля за деятельностью медицинских учреждений государством и страховыми компаниями, давать общие статистические данные. Данная система позволит четко выделять основные наиболее важные моменты, анализируя ситуации в целом, то есть отвечаю основному девизу врачей «Лечить человека, а не диагноз». Очень важным является то, что при моделировании исчезают рамки, установленные определенной медицинской школой, классификацией или особенностями страны. Что реально позволяет организовать сеансы телемедицины без границ в соответствии с рекомендациями Всемирной Организацией Здравоохранения.

Еремичев Даниил, отвечающий за налоговую службу, предлагает информатизацию налоговой сферы. Основной задачей внедрения инновационных технологий в налоговую сферу является информатизация всей структуры налоговых органов: создание основного вычислительного центра (ОВЦ), ЭВМ обладающего огромной вычислительной мощностью с

использованием технологий, основанных на нейронных сетях, дата-центра с большим потенциальным объемом данных и доступным ОВЦ, также создание оптоволоконной сети связывающей ОВЦ и дата-центр для достижения максимальной скорости передачи данных, создание наиболее защищенной сети между всеми офисами налоговой службы.

Заключение. Прогресс развития человеческих технологий не стоит на месте. С каждым днём человечество создаёт своё будущее и мы с каждым днём приближаемся к большой мечте - к реализации "Умного города". Цель этой мечты повышение качества жизни жителей городов и обеспечение устойчивого развития экономики. Широкое использование передовых информационно-коммуникационных технологий также призвано обеспечить интенсивное и качественное взаимодействие граждан, представителей бизнеса и органов власти.

СПИСОК ЛИТЕРАТУРЫ

1. Игнатьев М.Б. Просто кибернетика. — СПб. Страта: 2016 год. — 187 с.
2. Официальный сайт Администрации Санкт-Петербурга // https://gov.spb.ru/press/governor/110988/

УДК 519.8

МЕТОДОЛОГИЧЕСКИЕ И МЕТОДИЧЕСКИЕ ОСНОВЫ СОЗДАНИЯ И ПРИМЕНЕНИЯ КАТАСТРОФОУСТОЙЧИВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Охтилев Михаил Юрьевич[1], Ключарев Александр Анатольевич[1], Соколов Борис Владимирович[2], Юсупов Рафаэль Мидхатович[2]

[1]Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения»
Россия, Санкт-Петербург, 190000, Санкт-Петербург, ул. Большая Морская, 67, лит.А

[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39

e-mails: oxt@mail.ru, ak@aanet.ru, sokol@iias.spb.su, yusupov@iias.spb.su

Аннотация. В докладе предлагаются разработанные авторами научные основы формального описания и решения проблемы многокритериального структурно-функционального синтеза облика катастрофоустойчивых информационных систем. Приводятся примеры решения ряда практических задач создания и использования указанных информационных систем для различных предметных областей.

Ключевые слова: *комплексное моделирование; проактивное управление; многокритериальный структурно-функциональный синтез; катастрофоустойчивая информационная система.*

METHODOLOGICAL AND METHODICAL BASES OF CREATION AND APPLICATION OF DISASTER TOLERANT INFORMATION SYSTEMS

Okhtilev Mikhail[1], Klucharev Alecsandr[1], Sokolov Boris[2], Yusupov Rafael'[2]

[1]St. Petersburg State University of Aerospace Instrumentation
Russia, 190000, St. Petersburg, Bolshaya Morskaya str.,67A

[2] St. Petersburg Institute of Informatics and Automation, Russian Academy of Sciences
Russia, 199178, St. Petersburg, 14thline, 39

e-mails: oxt@mail.ru, ak@aanet.ru, sokol@iias.spb.su, yusupov@iias.spb.su

Abstracts: The report proposes the scientific basis for the formal description and solution of the problem of multicriteria structural-functional synthesis of the appearance of disaster-tolerant information systems developed by the authors. Examples are given of solving a number of practical problems of creating and using these information systems for different subject areas

Keywords: *complex modeling; proactive management; multi-criteria structural-functional synthesis; disaster-tolerant information system.*

Анализ существующих и прогнозируемых кризисных и чрезвычайных ситуаций, повсеместно возникающих в настоящее время в различных предметных областях, показывает, что они перестают быть отраслевыми, а перерастают в аварии и катастрофы, имеющие уже межотраслевой характер. В этих условиях исследовать и решать задачи повышения катастрофоустойчивости как бизнес-процессов, так информационных систем (ИС), обеспечивающих их выполнение, необходимо уже в рамках междисциплинарного подхода, интерпретируя их как задачи проактивного управления структурной динамикой (УСД) указанными процессами и системами. Предлагаемые докладе методологические и методические основы ориентированы на решение актуальной фундаментальной проблемы комплексной автоматизации и интеллектуализации процессов адаптивного структурно-функционального синтеза и

проактивного управления развитием катастрофоустойчивых ИС (КАИС) на основе скоординированной и обоснованной разработки и реализации полимодельного, многокритериального подхода к описанию исследуемой предметной области, а также создания и использования комбинированных методов и алгоритмов как для анализа свойств исследуемых процессов, так и для синтеза соответствующих программ и законов управления ИС в условиях динамично изменяющейся обстановки.

Содержание доклада. Предлагаемые в докладе методологические основы решения рассматриваемой проблемы базируются на четырех базовых концепциях, к числу которых отнесены концепции комплексного моделирования и проактивного управления, концепция инвариантности реальных и вычислительных процессов, их описывающих, а также концепция интеллектуализации процессов формирования и реализации управленческих процессов [1, 2].

При этом в докладе под комплексным (системным) моделированием (КМ) сложных объектов (СлО) любой природы (естественных, искусственных, реально существующих и виртуальных и т.п.), к числу которых относятся и ИС, понимается методология и технологии полимодельного описания указанных объектов, а также комбинированного использования методов, алгоритмов и методик многокритериального анализа, синтеза и выбора наиболее предпочтительных управленческих решений, связанных с созданием, использованием и развитием рассматриваемых объектов в различных условиях динамически изменяющейся внешней и внутренней обстановок. В свою очередь, проактивное управления КАИС на различных этапах их жизненного цикла в отличие от традиционно используемого реактивного управления СлО, ориентированного на оперативное реагирование и последующее недопущение инцидентов, предполагает предотвращение возникновения инцидентов за счет создания в соответствующей системе мониторинга и управления принципиально новых прогнозирующих и упреждающих возможностей при формировании и реализации управляющих воздействий, базирующихся на концепции системного (комплексного) моделирования.

Предложена оригинальная обобщенная методика решения задач комплексного планирования модернизации и функционирования ИС в условиях динамично изменяющейся обстановки, которая включает две основные фазы. На первой фазе должно осуществляться формирование (генерирование) допустимых вариантов многоструктурных макросостояний ИС или, говоря другими словами, оперативный структурно-функциональный синтез нового облика ИС, соответствующего целям проводимой модернизации и складывающейся (прогнозируемой) обстановке, связанной с возможной деградацией структур создаваемой и существующей КАИС.

На второй фазе проводится выбор конкретного варианта многоструктурного макросостояния КАИС с одновременным синтезом (построением) адаптивных комплексных планов (программ) управления переходом КАИС из текущего в требуемое (выбранное) макросостояние.

В докладе приводятся примеры практической реализации полученных научных результатов при создании и применении КАИС в различных предметных областях (космонавтика, атомная энергетика, логистика, военное дело) [2].

Заключение. Предлагаемое в докладе рассмотрение вопросов комплексного адаптивного планирования и управления модернизацией и функционированием катастрофоустойчивых ИС в общем контексте проактивного управления их структурной динамикой позволяет, во-первых, непосредственно связать те общие цели, на достижение которых ориентировано функционирование конкретной бизнес-системы (БС) и соответствующей КАИС, с теми целями, которые реализуются в ходе управления структурами БС и ИС, во-вторых, обоснованно определить и выбрать соответствующие последовательности решаемых задач и выполняемых операций (действий), связанных со структурной динамикой (другими словами, синтезировать технологию управления как БС, так и КАИС), и, в-третьих, осознанно находить компромиссные решения при распределении ограниченных ресурсов, выделяемых на управление структурной динамикой указанных систем в условиях возможных кризисных, чрезвычайных и аварийных ситуаций.

Исследования, выполненные по данной тематике, проводились при финансовой поддержке ведущих университетов Российской Федерации: СПб ГПУ (мероприятие 6.1.1), ИТМО (субсидия 074–U01), Программы НТС Союзного государства «Мониторинг-СГ» (проект 1.4.1-1), грантов РФФИ (№№15-07-08391, 15-08-08459, 16-07-00779, 16-08-00510, 16-08-01277, 16-29-09482-офи-м, 17-08-00797, 17-06-00108, 17-01-00139), госзадания Министерства образования и науки РФ №2.3135.2017/4.6, в рамках бюджетных тем №№0073–2014–0009, 0073–2015–0007, Международного проекта ERASMUS +, Capacity building in higher education, № 73751-EPP-1-2016-1-DE-EPPKA2-CBHE-JP.

СПИСОК ЛИТЕРАТУРЫ

1. Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. М.: Наука, 2006. 410 с.
2. Технология системного моделирования / Е.Ф. Аврамчук, А.А. Вавилов, С.В. Емельянов и др.; Под общ. ред. С.В. Емельянова и др. – М.: Машиностроение; Берлин: Техника, 1988.

УДК 378.1

НООСФЕРНОЕ ОБРАЗОВАНИЕ В РАЗВИТОМ ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Советов Борис Яковлевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Россия, Санкт-Петербург, ул. Профессора Попова, 5
e-mail: bysovetov@mail.ru

Аннотация. Текущий век войдет в историю человечества как век информатизации, век завершения построения информационного общества во всем мире. В начале века было трудно предсказать содержание и этапы становления информационного общества, виды и возможности информационных технологий. За истекшие годы этого столетия удалось перейти к завершающему этапу построения информационного общества, однако проблема приоритетности образования в информационном обществе, сформулированная еще в 1992 году, оказалось до настоящего времени не решенной. В то же время уже в настоящее время представляется возможным реализовать идею В.И. Вернадского о ноосферном разуме на новой неизвестной ранее основе – на базе единого информационного пространства с использованием новых информационных технологий. Завершающий (третий) этап построения информационного общества нацелен на объединение персональных информационных фондов в единый мировой фонд, возможности которого в дальнейшем могут стать неисчерпаемы. Это изменяет подход к целям и реализации образовательной системы любой страны, предоставляя уникальные возможности формирования и использования новых знаний в обществе. Для информационного общества характерна лидирующая роль образования, а поэтому будущее образования следует рассматривать в тесной взаимосвязи с особенностями жизни людей в информационном обществе. При этом особо важна ориентация образования на нравственные цели, приоритет духовной составляющей перед материальной, что станет основой подхода к формированию мировой системы ноосферного образования и приведет к кардинальным изменениям государственной политики в сфере образования.

Ключевые слова: *ноосферное образование; развитое информационное общество; мировой информационный фонд образования.*

NOOSPHERE EDUCATION IN THE DEVELOPED INFORMATION SOCIETY

Sovetov Boris
St. Petersburg State Electrotechnical University «LETI»
Russia, St. Petersburg, Professor Popov str., 5
e-mail: bysovetov@mail.ru

Abstract. The current century will become history of mankind as a century of informatization, a century of completion of creation of information society around the world. At the beginning of the century it was difficult to predict the content and stages of formation of information society, types and possibilities of information technologies. For the expired years of this century it was succeeded to pass to the final stage of creation of information society, however the problem of priority of education in information society formulated in 1992 it was not solved so far. At the same time already now it is obviously possible to basis to realize V.I. Vernadsky's idea about noosphere mind on the new unknown earlier – on the basis of a common information space with use of new information technologies. The finishing (third) stage of creation of information society is aimed at merging of personal information funds in uniform world fund which possibilities can become inexhaustible further. It changes approach to the purposes and realization of educational system of any country, giving unique opportunities of formation and use of new knowledge in society. The leading education role and therefore the future of education should be considered in close interrelation with features of life of people in information society is characteristic of information society. At the same time orientation of education to the moral purposes, a priority of a spiritual component before material is especially important that it will become a basis of approach to formation of world system of noosphere education and will lead to cardinal changes of state policy in education.

Keywords: *noosphere education; the developed information society; world information fund of education.*

Идеи ноосферного этапа в развитии человечества были выдвинуты В.И. Вернадским. Однако в начале прошлого века трудно было предвидеть будущее возникновение и развитие нового научного направления – информатики. А соответственно не представлялась возможной реализация объединения знаний в мировом масштабе. В 1947 г. К. Шеннон в работе «Статистическая теория связи» заложил теоретические основы передачи дискретных сообщений, сформулировав фундаментальные теоремы, определившие условия передачи сообщений по дискретным каналам связи без шума и с шумом при различных соотношенияхсм производительности источника и пропускных способностях канала связи. Этим было положено начало развитию теории передачи сообщений по каналам связи и впоследствии научному направлению – информатике. В настоящее

время информатика может рассматриваться на трех уровнях: нижнем – базовом, в виде средств вычислительной техники и техники связи, среднем – формальном, в виде совокупности информационных технологий и верхнем – реализационном, в виде прикладных информационных систем. Все уровни динамично развиваются и активно внедряются в жизнь общества.

К. Шеннон предсказал бурное развитие информационных технологий и определил 21-й век как век информатики. Еще в девяностые годы прошлого века на государственном уровне была сформулирована задача построения нового общества – общества информационного. В начале текущего века были разработаны концепция, программа и стратегия перехода в информационное общество. За истекший период реализованы программы информатизации образования, программа развития информационного общества и ряд других федерального и отраслевого значения, направленных на информатизацию деятельности органов представительной и исполнительной власти.

Создание информационного общества – это политическая, экономическая и культурная цель во многих рыночных экономиках. Движение к этой цели стимулируется национальными стратегическими программами, программами развития и большим числом различных других инициатив. Ведутся тысячи международных, национальных, региональных и местных проектов. Информационное общество является наиболее привлекательным и многообещающим направлением деятельности в сегодняшние бурные времена. Все государства, принявшие Стратегии перехода в информационное общество, имеют строгие политические обязательства в этом направлении.

Концепция информационного общества довольно абстрактна. Нет общепринятого определения этого термина, который сформировался на основе понятий: «инфодеревня» в Японии, и «telematics» во Франции. Хотя рыночные экономики ряда стран уже фактически достаточно продвинуты в части развития информационного общества, многие концепции по своей сути футуристичны и ориентированы на технологии. Это объясняется тем, что быстрое развитие информационно-коммуникационных технологий (ИКТ) коренным образом изменило различные виды бизнеса и услуг – интенсивно формируется «общество информационных технологий». По современным воззрениям информационное общество – это такое общество, в котором производство и потребление информации является важнейшим видом деятельности, а информация признается наиболее значимым ресурсом, новые информационные и телекоммуникационные технологии и техника становятся базовыми технологиями и техникой, а информационная среда наряду с социальной и экологической – новой средой обитания человека.

Стратегия формирования информационного общества предполагала наличие трех этапов: этапа компьютеризации, этапа формирования информационной инфраструктуры (на базе единой телекоммуникационной среды) и этапа объединения индивидуальных информационных фондов в единый мировой информационный фонд с удаленным доступом каждого члена общества к этому ресурсу. Завершающий этап построения информационного общества реализует конструктивно идею Вернадского о ноосфере, так как формируется единый информационный фонд человечества, включающий совокупность знаний, объединяемых мировым информационным пространством. Создается реальная предпосылка перехода к обществу знаний. В этих условиях образование действительно должно занять приоритетное место и гармонично наполниться ноосферной идеологией в части целей, содержания, организации и результатов. В информационном обществе образование приобретает лидирующую роль. Информационные технологии пронизывают все стороны жизни и деятельности людей. Экономика становится цифровой, решается задача цифровой трансформации управления в органах государственной власти.

Информационное пространство Российского образования сливается с мировым образовательным пространством. При этом оно должно отвечать национальным интересам и базироваться на традициях отечественной культуры. В противном случае молодое поколение попадает под влияние информационной среды, чуждой нашим интересам и зачастую преследующей корыстные цели. Ноосферность образования предполагает в процессе обучения формирование нового мировоззрения, обеспечивающего комфортное проживание человека в обществе знаний.

Проблема развития интеллектуальных способностей личности смыкается уже сейчас с проблемой информатизации образования. Информатизация должна предусматривать эволюционное развитие методологии образования. Не отрицание, а последовательное эволюционное развитие сложившейся методологии образования за счет использования явных преимуществ компьютерных технологий (наглядность, возможность использования различных форм представления информации - звук, изображение, удаленный доступ, обработка и хранение больших объемов информации) должно стать основой опережающего развития образования. Информатизация внесла существенные изменения в структуру и организацию учебного процесса. Реализуется дистанционное обучение, формируется электронная образовательная среда, видоизменился документооборот. Возникла и успешно реализуется идея контроля деятельности образовательных организаций по содержанию их сайтов. Таким образом, информатизация позволила перевести на новый современный уровень управление образованием и существенно изменить формы организации учебного процесса.

В рамках федерального государственного образовательного стандарта (ФГОС) высшего образования предусмотрены возможности от включенного дистанционного обучения до сетевого взаимодействия вузов с обменов имеющихся ресурсов. Вступившие в действие ФГОС высшего

образования позволяют в условиях сохраняющейся квазиадминистративной модели организации образования реализовать отдельные элементы либеральной модели, характерной для уровневой подготовки за рубежом. Базовая квазиадминистративная модель образования, действующая в российской высшей школе, обладает следующими особенностями:

а) профессиональная квалификационная структура подготовки специалистов определяется перечнем укрупненных направлений подготовки и специальностей;

б) по всем направлениям и специальностям разрабатываются ФГОС;

в) ВУЗы могут выдавать дипломы установленного (государственного) образца после аккредитации;

г) образовательный процесс возможен после получения лицензии.

В условиях современной рыночной экономики выпускнику необходимо предоставить свободу в выборе образовательной траектории и последующего места работы. По сути, это приводит к замене базовой квазиадминистративной модели на либеральную. Можно выделить следующие особенности либеральной модели:

а) академические свободы и автономии университетов;

б) возможность самостоятельно модернизировать образовательные программы;

в) открытие новых образовательных программ без разрешения Министерства;

г) классификация образовательных программ сопоставима с Международной стандартной классификацией образования.

Особенно важно на современном этапе образования врамках действующих ФГОС воспитать у выпускника способность адаптироваться в сложных рыночных условиях с ориентацией всего общества на нравственные ценности. Нужно вернуться к лучшим традициям российского образования, отдавая приоритет воспитанию перед обучением. Эту проблему необходимо решать на основе формирования соответствующих компетенций (в том числе, ноосферного характера), которые заложены в основу построения ФГОС высшего образования. Особо важно сохранить лучшие традиции русского просвещения и отечественного образования. В условиях действия санкций со стороны западных государств и решения проблемы импортозамещения необходимо переориентировать вектор российского образования на подготовку специалистов, удовлетворяющих требованиям работодателя. В соответствии с этим следует наряду с подготовкой бакалавров и магистров вернуться к специалитету, понятному работодателю и способному в полной мере реализовать импортозамещение. При этом полезно осуществить гибкий уход от уровневой системы образования западного образца, совмещая на младших курсах обучения в вузе разные образовательные траектории для выявления способностей и наклонностей обучаемых. При сохранении на отдельных направлениях уровневой подготовки необходимо ограничиться двумя уровнями, вернув аспирантуру в статус научной структуры с обязательной защитой диссертации после ее завершения.

Даже в условиях многоуровневой системы образования существуют предпосылки для введения ноосферной составляющей в процесс подготовки кадров. Прежде всего, необходимо формировать ноосферное мировоззрение у преподавателей, что в современных условиях при подходе к образованию как к услуге сделать непросто. Нелегко сменить существующую в настоящее время ориентацию образования на успешность, его направленность на решение сиюминутных задач на ноосферное образование, ориентированное на достижение нравственных идеалов Недопустимы уход от фундаментализации образования, замена сложившихся фундаментальных дисциплин, новыми, зачастую непонятными по целям и содержанию. Ноосферность образования предполагает овладение отечественной культурой, родным языком, классической литературой, музыкой и искусством. Необходимо в подрастающем поколении поддерживать интерес к нравственным ценностям. Содержательно в рамках либеральной модели образования следует более решительно вводить компетенции ноосферного характера, что позволит предложить новый набор дисциплин, способствующих нравственному развитию обучаемых.

Наступает этап развитого информационного общества, который должен перейти в этап интеллектуального общества. Цифровизация экономики, удаление операторов из сферы экономических (в том числе, банковских) операций потребует нового подхода к развитию и использованию информационных технологий. Необходима дальнейшая интеграция образования, науки и промышленности при совершенствовании уже оправдавших себя формах интеграции, таких как: базовые кафедры, отраслевые лаборатории, научно-образовательные центры, технопарки, бизнес инкубаторы. Потребуются разработка систем искусственного интеллекта, внедрение роботов во все сферы производства и потребления. При этом не должен быть подавлен естественный интеллект. Эти задачи могут решить специалисты, обладающие ноосферным образованием, которое должно формироваться уже в настоящее время, и для этого имеются все необходимые условия на завершающем этапе развития информационного общества.

СПИСОК ЛИТЕРАТУРЫ

1. Б.Я. Советов, В.В. Касаткин. Новые тенденции подготовки кадров в области информационных технологий (пленар. доклад) // Перспективные направления развития отечественных информационных технологий: материалы II межрегиональной научно-практическая конф. Севастополь, 13-17 сентября 2016 г. / Севастопольский государственный университет; науч. ред. Б.В. Соколов - Севастополь: СевГУ, 2016.
2. Советов Б.Я. Тенденции развития высшего образования и подготовки кадров в области информационных технологий. // Региональная информатика (РИ-2016). Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». Санкт-Петербург, 26-28 октября 2016 г.: Материалы конференции. / СПОИСУ. – СПб., 2016. – 599 с.

УДК 33+629.78+528

ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ КОСМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В ИНТЕРЕСАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Усатый Вадим Анатольевич, Ющенко Сергей Петрович
Юго-западный государственный университет
Россия, Курск, ул. 50 лет Октября, 94
e-mail: kafedra.ist2015@yandex.ru

Аннотация. В статье рассмотрены проблемы использования результатов космической деятельности для информационной поддержки принятия решений органами регионального и муниципального управления на территориях субъектов Российской Федерации. Показано, что в условиях рыночной экономики, привлечения крупных, в том числе зарубежных инвесторов для развития предприятий и отраслей экономики, нерешенность этих проблем определяет возникновение угроз информационно-экономической безопасности российских регионов.

Ключевые слова: *информационно-экономическая безопасность; регионы РФ; результаты космической деятельности; эффективность.*

APPLICATION OF SPACE ACTIVITY RESULTS IN THE INTERESTS OF PROVIDING INFORMATION AND ECONOMIC SECURITY IN RUSSIAN FEDERATION REGIONS

Usaty Vadim, Iushchenko Sergei
South-west state university
Russia, Kursk,50 let Oktabrja, 94
e-mail: kafedra.ist2015@yandex.ru

Abstract. The paper presents the issues related to application of space activity results in order to provide information support for decision-making purposes of regional and municipal authorities on the territory of Russian Federation. The paper shows that in current competitive environment when large Russian and foreign investors are to be drawn to the development of enterprises and branches of economy the fact that these issues remain unsolved causes information and economic security risks in Russian regions.

Keywords: *information and economic security; RF regions; results of space activity; performance.*

В последние годы в условиях интенсивного развития космической техники наблюдается резкое возрастание масштабов использования данных дистанционного зондирования Земли (ДЗЗ), спутниковых навигационных определений и других результатов космической деятельности (РКД) для информационной поддержки процессов управления государствами и регионами. Высокая оперативность получения данных ДЗЗ, их достоверность, высокая детальность, возможность одномоментного охвата значительных территорий и т.п. обеспечивает наиболее развитым странам стратегическое информационное превосходство не только в политической и военной, но и в экономической сфере. Кроме того, доступность и уже достаточно приемлемая стоимость РКД обеспечивают коммерческим организациям широкие возможности для получения сведений, характеризующих направленность и результаты экономической деятельности потенциальных конкурентов в любых странах мира.

Вместе с тем использование РКД для информационной поддержки деятельности региональных и муниципальных органов управления на территориях субъектов РФ еще не в полной мере соответствует требованиям, достигнутому уровню развития науки и космической техники. В условиях рыночной экономики, необходимости привлекать зарубежных инвесторов для развития предприятий и отраслей экономики, указанное обстоятельство часто влечет возникновение угроз информационно-экономической безопасности российских регионов [1]. В этой связи ниже рассмотрены основные проблемы широкомасштабного использование РКД в органах управления российских регионов.

К числу субъектов РФ, где работы по использованию РКД в информационных системах региональных и муниципальных органов управления ведутся наиболее продуктивно, сегодня относится Курская область. Здесь еще в начале 2000-х годов широким фронтом были развернуты работы по рассматриваемой проблематике, проведены исследования особенностей информационного обеспечения национальной безопасности РФ на региональном уровне, информационной поддержки этих процессов с использованием новых информационных технологий [2].

В ходе выполнения этих работ подтверждена достаточно высокая эффективность использования РКД для решения задач управления каждодневной жизнедеятельностью регионов и территорий. Их использование обеспечивает, например:

- увеличение числа выявленных экологических правонарушений до 2-х раз;
- рост налоговых поступлений за пользование ресурсами на 15 – 45%, недрами на 5 – 15%;

– сокращение сроков выполнения работ по учету земель и недвижимости до 3-х раз, увеличение поступления земельных платежей на 35 – 45%;

– сокращение до 2-х раз сроков на выполнение работ по созданию объектов инфраструктуры, затрат на их проведение на 20 – 30%;

– снижение затрат на ликвидацию аварий и возникающих чрезвычайных ситуаций на 10 – 20% и т.д.

Вместе с тем, полученный к настоящему времени опыт позволил сформулировать ряд проблем широкомасштабного использование РКД, которые представляются типовыми при обеспечении информационно-экономической безопасности большинства российских регионов. К основным из них отнесены:

– неполнота нормативно-правовой базы, регламентирующих порядок предоставления РКД федеральными министерствами и ведомствами (федеральным оператором) при функционировании региональных и муниципальных органов управления в режиме «каждодневная деятельность», а также «угроза возникновения ЧС в отрасли экономики или на территории субъекта РФ», «чрезвычайная ситуация»;

– отсутствие «линейки» отечественных сертифицированных аппаратно-программных средств, обеспечивающих комитетам и службам региональных и муниципальных органов управления возможность оперирования РКД при решении соответствующих задач социально-экономического развития субъектов РФ, управления жизнедеятельностью регионов;

– отсутствие государственных решений, регламентирующих порядок перехода федеральных, региональных и муниципальных органов управления РФ к оперированию РКД в системах координат «Параметры Земли 1990 года» и «Геодезическая система координат 2011 года»;

– отсутствие системы подготовки бакалавров, специалистов и магистров по направлению «Использование РКД в системах менеджмента организаций», переподготовки и повышения квалификации сотрудников региональных и муниципальных органов управления по этому направлению;

– недостаточная разработка научно-методических основ оценивания экономической эффективности использования РКД в управлении процессами социально-экономического и инвестиционного развития субъектов РФ и т.д.

Решение первой из указанных проблем требует проработки механизмов формирования региональными органами управления на территориях субъектов РФ заявок на РКД, а также их выполнения федеральным оператором с учетом различий в приоритетах, требуемой оперативности предоставления данных и т.п. Так, например, в режиме «каждодневная деятельность» на выполнение заявки допустимо отводить недели и месяцы, а в режиме «чрезвычайная ситуация» материалы ДЗЗ на требуемые территории должны быть получены в течение нескольких часов, максимум суток.

При этом представляется, что на федеральном уровне для органов регионального и муниципального управления должен быть один источник получения требуемых РКД, включая данные ДЗЗ как от отечественных, так и от зарубежных космических аппаратов (в том числе коммерческих), а механизм получения требуемых данных должен быть достаточно «прозрачным». Другими словами, органы регионального и муниципального управления не должны задумываться о возможных источниках получения РКД: будь то Научный центр оперативного мониторинга Земли, другие отечественные или зарубежные операторы, в задачи которых входит, например, предоставление материалов космической съемки местности в рамках Международной Хартии по космосу и крупным катастрофам.

Система обеспечения РКД должна функционировать таким образом, чтобы органы регионального и муниципального управления формулировали только требования к РКД, включая границы района съемки местности, требуемый уровень разрешения, спектральный диапазон, ожидаемые сроки предоставления данных, уровень их обработки и т.п.

С этой целью в регионе, возможно, должен быть создан региональный оператор, либо его функции могут быть возложены на так называемые Центры космических услуг, созданные примерно в 50-и субъектах РФ. На подобного оператора должны быть возложены и функции хранения всех поступивших в регион данных съемки местности и других РКД. При необходимости он же должен быть способен организовать съемку требуемых участков местности в регионе с использованием авиации или БПЛА, а также осуществлять наиболее сложные виды тематической обработки материалов съёмки местности в интересах комитетов и служб региональных и муниципальных органов управления, не обладающих такой возможностью.

Вторая из проблем связана с тем, что в комитетах и службах региональных и муниципальных органов управления субъектов РФ сегодня установлено и используется программное обеспечение для работы с РКД различных отечественных и зарубежных производителей.

Более того, в последние годы комитеты и службы финансируют разработки такого программного обеспечения, исходя из собственных представлений о его предназначении и требуемых функциональных возможностях. Очевидно, что при этом часто используются специфические форматы представления геопространственных и атрибутивных данных, различные подходы к их визуализации и обработке, зарубежные системы координат и т.п.

Сложившееся положение существенно затрудняет организацию обмена данными между комитетами и службами, является сдерживающим фактором отображения разнородных данных об

обстановке на территориях и в отраслях экономики субъектов РФ, затрудняет организацию информационного взаимодействия Ситуационных центов глав администраций субъектов РФ с информационными системами федеральных министерств и ведомств, включая Национальный центр управления в кризисных ситуациях, Национальный центр управления обороной страны.

Представляется целесообразным создание «линейки» отечественных сертифицированных программных средств, ориентированных на работу с материалами аэрокосмической съемки местности и другими РКД в интересах решения задач, стоящих перед региональными и муниципальными органами управления.

Наличие такой «линейки» позволило бы «конфигурировать» безызбыточные по своим функциональным возможностям (а потому, сравнительно недорогие) комплексы программных средств, исходя из тех прикладных задач, которые региональным и муниципальным органам управления приходится реально решать с использованием РКД: просмотр материалов съемки отдельных участков местности и тематических слоев; отображение поступающих навигационных определений и оперирование ими; создание тематических геопространственных данных и их занесение в региональное хранилище; 3-х мерная визуализация объектов и территорий; работа с материалами лазерного сканирования объектов и участков местности; создание псевдореалистических изображений городской застройки; тематическая обработка материалов гиперспектральной съемки местности и т.п.

Программные компоненты такой «линейки», наряду с адекватной стоимостью, должны быть рассчитаны на различный уровень подготовки пользователей, предусматривать централизованное обновление, обеспечивать возможность доработки под специфические нужды региональных и муниципальных органов управления на той или иной территории РФ. Для удаленных регионов должна обеспечиваться возможность дистанционного обслуживания программных компонентов такой «линейки», системного администрирование и т.п.

Третья из рассматриваемых проблем связана с недостаточной регламентацией порядка перехода федеральных, региональных и муниципальных органов управления РФ к оперированию РКД с использованием государственных систем координат «Параметры Земли 1990 года» и «Геодезическая система координат 2011 года».

Как известно, к настоящему времени в федеральных, региональных и муниципальных органах управления РФ, организациях и ведомствах имеется огромный объем геопространственных данных, представленных в различных форматах и системах координат. И каким образом обеспечивать их оперативное извлечение из ведомственных баз данных, совместное отображение, обработку и последующее использование пока не вполне понятно.

Одним из путей решения этой проблемы являются начатые в РФ работы по созданию для федеральных, региональных и муниципальных органов управления единой электронной координатной основы для представления геопространственных данных и навигационных определений в государственных системах координат «Параметры Земли 1990 года» и «Геодезическая система координат 2011 года». Вместе с тем преобразование, приведение к этой единой электронной координатной основе десятилетиями накапливавшихся разнородных геопространственных данных представляет собой достаточно сложную задачу, пути решения которой не всегда являются тривиальными.

Четвертая проблема – отсутствие в вузах страны системы подготовки бакалавров, специалистов и магистров по направлению «Использование результатов космической деятельности в системах менеджмента организаций», а также переподготовки и повышения квалификации сотрудников региональных и муниципальных органов управления, оперирующих РКД. Без ее решения самые лучшие аппаратно-программные комплексы для работы с РКД, установленные в комитетах и службах региональных и муниципальных органов управления остаются невостребованными.

Решение этой проблемы требует согласованных усилиях Министерства образования и науки, Министерства труда и социальной защиты РФ, а также ведущих ВУЗов страны в части организации разработки образовательного стандарта по направлению «Использование результатов космической деятельности в системах менеджмента организаций», комплекта соответствующих профессиональных стандартов, учебно-методических материалов для подготовки специалистов по указанному направлению в ВУЗах и средне-технических учебных заведениях страны, переподготовки и повышения квалификации сотрудников региональных и муниципальных органов управления на территориях субъектов РФ, оперирующих РКД.

Пятая проблема связана с недостаточной проработанностью научно-методических основ оценивания экономической эффективности использования РКД в управлении процессами социально-экономического развития, повышения инвестиционной привлекательности субъектов РФ.

В прошлые годы, до тех пор, пока работа с данными ДЗЗ и навигационными определениями в региональных и муниципальных органах управления оставалась экзотикой, никто денег не считал. Проводились те или иные разрозненные исследования. И, если в их ходе удавалось что-то сделать - уже было хорошо. А с какими финансовыми затратами был поучен результат – тогда никого не интересовало.

Сегодня мы перешли к этапу широкомасштабного использования РКД практически во всех сферах жизнедеятельности страны и ее регионов. Поэтому особую актуальность приобретает планирование финансовых затрат на использование РКД при решении задач регионального и муниципального управления, получение оценок потенциальных эффектов от их использования. Необходимо научиться не только оперировать РКД при решении задач регионального и муниципального управления, но и оценивать экономическую эффективность их использования. В этом плане необходимы усилия наших ученых РАН и прикладных НИИ, профессорско-преподавательского состава «экономических» кафедр ведущих ВУЗов страны.

Завершая рассмотрение проблем использования РКД для информационной поддержки деятельности региональных и муниципальных органов управления отметим, что почти 20-и летний опыт выполнения работ в Курской области свидетельствует, что их решение возможно только при скоординированных усилиях федеральных, региональных и муниципальных органов управления РФ, организаций РАН и ВУЗов страны.

Преимуществом комплексного подхода является концентрация усилий государственных и муниципальных органов управления, организаций науки и ВУЗов страны на наиболее актуальных проблемных вопросах использования РКД потенциала для дальнейшего социально-экономического развития страны и ее регионов.

Рассмотренные и другие предложения по решению проблем использования РКД для информационной поддержки деятельности региональных и муниципальных органов управления представлены в систематизированной виде [3] в Правительство РФ для использования при разработке перечня мер организационного, нормативно-правового и методического характера, предусмотренного Указом Президента РФ от 13.05.2017 г. №208 «О стратегии экономической безопасности Российской Федерации на период до 2030 года».

Экспертные оценки, полученные на основе анализа опыта выполненных работ в РФ и наиболее развитых странах мира, показали, что реализация этих предложений позволит:

– ускорить в 3-10 раз и снизить на 30-40% стоимость внедрения РКД в процессы социально-экономического развития российских регионов за счет разработки и последующего тиражирования типовых организационных и научно-технических решений, привлечения коммерческих структур к решению задач информационного обеспечения деятельности региональных и муниципальных органов управления с использованием РКД;

– инициировать процесс формирования в РФ рынка космических услуг, объединения его с профильными рынками по принципу удовлетворения аналогичных (смежных) рыночных потребностей;

– в течение ближайших 2-3 лет повысить на 60-70 % спрос на РКД в региональных и муниципальных органах управления, отраслях экономики, коммерческих структурах, довести до 25-30% долю коммерческих организаций в объеме финансовых средств, привлекаемых в интересах использования РКД для социально-экономического развития РФ и ее регионов;

– повысить привлекательность космоса как одной из отраслей российской экономики, повысить престиж и авторитет страны на международной арене;

– активизировать и оптимизировать процессы использования РКД в интересах обеспечения национальной безопасности РФ, дальнейшего ее социально-экономического развития, обеспечения безопасности жизнедеятельности населения.

Таким образом, в настоящее время в информационном обеспечении процессов принятия решений региональными и муниципальными органами управления на территориях субъектов РФ существует ряд типовых проблем широкомасштабного использование РКД. Их наличие влечет возникновение угроз информационно-экономической безопасности, является сдерживающим фактором социально-экономического и инвестиционного развития российских регионов. С учетом опыта работ, выполненных в Курской области, рассмотрены пути их решения, предусматривающие скоординированную деятельность федеральных и региональных органов власти в части организации информационной поддержки процессов управления жизнедеятельностью регионов.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).
2. Ющенко С.П. Многоагентные системы информационной поддержки управленческих решений. — Ростов-на-Дону: Из-во СКНЦ ВШ, 2004 — 376 с.
3. Усатый В.А., Шабанов А.В., Ющенко С.П. Проблемы организации информационной поддержки деятельности органов регионального и муниципального управления субъектов РФ с использованием результатов космической деятельности// VI Среднерусский экономический форум, 16-17 июня 2017 г, Курск. Материалы заседания «круглого стола». Из-во ЮЗГУ, 2017. С. 10-22.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

УДК004.056

ДИАГНОСТИРОВАНИЕ НАРУШЕНИЙБЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Авраменко Владимир Семенович, Маликов Альберт Валерьянович
Военная академия связи им. Маршала Советского СоюзаС.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: vsavr@yandex.ru, mkv.vas@yandex.ru

Аннотация. Рассмотрен подход к решению задачи диагностирования нарушений безопасности в инфокоммуникационных системах с применением аппарата искусственных нейронных сетей. Проанализирована возможность повышения эффективности диагностирования нарушений безопасности и пути ее реализации.

Ключевые слова: *диагностирование; искусственные нейронные сети; обнаружение атак; SIEM-системы.*

DIAGNOSTICS OF INFRINGEMENTSOF INFORMATION SECURITY BASED ON ARTIFICIAL NEURAL NETWORKS IN INFORMATION AND COMMUNICATION SYSTEMS

Avramenko Vladimir, Malikov Albert
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: vsavr@yandex.ru, mkv.vas@yandex.ru

Abstract. The article presents approach to solving the problem of diagnosing security breaches in information and communication systems with application of artificial neural networks. Analyzed the possibility of increasing the efficiency of diagnosing security breaches and ways to implement it.

Keywords: *diagnosis; artificial neural network; attack detection; SIEM-systems.*

Многообразие форм негативных программно-технических воздействий на инфокоммуникационные системы способствовало развитию широкого спектра средств защиты информации. Но, даже успешно зафиксировав и отразив попытку несанкционированного воздействия с помощью системы обнаружения атак или средств антивирусной защиты, администратор безопасности не может быть уверен в том, что вторжение в подконтрольную ему зону ответственности остановлено и инцидент исчерпан. Требуется детальное диагностирование нарушения безопасности. Особенно актуальна задача диагностирования нарушений безопасности при обнаружении целенаправленных (таргетированных) атак, а также ранее неизвестных атак, в том числе, так называемых атак “нулевого дня”, для которых, как правило отсутствуют, готовые сценарии адекватного реагирования.

Под нарушением безопасности информации в инфокоммуникационной системе понимается событие, заключающееся в появлении или реализации угрозы безопасности информации, передаваемой, обрабатываемой или хранящейся в этой системе. В литературе и в нормативных документах также используется термин «инцидент информационной безопасности», под которым понимается появление одного или нескольких нежелательных, или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности.

Диагностирование нарушений безопасности информации представляет собой процесс сбора и анализа информации о нарушении безопасности информации с целью идентификации характеристик нарушений безопасности. К основным характеристикам нарушения можно отнести тип, цель (объект атаки), результат атаки, последствия (уровень риска, ущерб), способ реализации, идентификаторы, роли и местоположение участников нарушения, причины нарушения. На основе результатов диагностирования осуществляется выработка варианта реагирования на нарушения безопасности информации. В литературе понятию «анализу нарушений безопасности информации» в большей степени соответствуют понятия «оценка инцидента информационной безопасности», «расследование», а процессу выработки варианта реагирования на нарушения безопасности информации – процесс принятия решений по событиям/инцидентам.

Также диагностирование нарушений безопасности информации можно рассматривать как частную задачу мониторинга информационной безопасности в инфокоммуникационной системе [1]. В ходе мониторинга администратором на основе результатов диагностирования принимаются решения по управлению защитой в рамках общего процесса управления инфокоммуникационной системой [2].

Необходим комплексный подход к решению задачи диагностирования нарушений безопасности, при этом целесообразно анализировать данные не только из журналов событий всех имеющихся элементов атакованной сети, но и дополнительную информацию из других источников. Также целесообразно использовать базу знаний, содержащую сведения о ранее совершенных нарушениях, результатах их диагностирования и реагирования на них, для корреляционного анализа событий и получения новых знаний. Следует отметить, что задачу централизованного сбора информации от элементов инфокоммуникационной системы (в том числе и от средств защиты информации) и последующей ее нормализации и корреляциии решают активно развивающиеся SIEM-системы. При этом стоит учесть, что данные программно-аппаратные системы достаточно дороги, сложны в настройке, требуют высокой квалификации для создания правил реагирования, учитывающих особенности инфраструктуры защищаемой инфокоммуникационной системы организации.

При разработке математического обеспечения системы автоматизированного диагностирования нарушений безопасности информации (методов, моделей алгоритмов) могут использоваться методы и математический аппарат теории вероятностей и математической статистики, распознавания образов, нечетких множеств, биоинспирированные методы.

Одним из возможных путей повышения эффективности диагностирования нарушений безопасности является автоматизация основных функций диагностирования на основе аппарата искусственных нейронных сетей. Искусственные нейронные сети используются для решения задач распознавания образов, кластеризации, аппроксимации функций, прогноза, оптимизации, управления. При этом нейронная сеть способна с заданной достоверностью решать указанные выше задачи, используя для этого необходимое количество примеров.

С целью определения значений (оценки) характеристик нарушения, существенных для процесса принятия решения по реагированию на нарушение безопасности, полученные и предварительно обработанные данные от элементов инфокоммуникационной системы, поступают на вход искусственной нейронной сети. Получив на выходе нейросети значения характеристик и показателей нарушения безопасности, администратор принимает решение на реагирование.

Также нейронные сети могут быть применены в качестве дополнительного инструмента, повышающего эффективность обнаружения и диагностирования в существующих системах обнаружения компьютерных атак. В [3] показано как построенный на базе нейронной сети адаптивный модуль может функционально заменить систему обнаружения атак (нейросетевой модуль выполнял анализ заголовка сетевого пакета и семантический анализ его наполнения, при этом коэффициент соответствия, определяемый как отношение количества правильных ответов адаптивного модуля к количеству ошибок после обучения нейросети, составил 0,8).

Эффективность диагностирования может быть повышена путем решения задачи поиска характеристик нарушений безопасности, скрытых в больших объемах разнородной информации на основе технологии Data Mining, реализуемой на базе искусственных нейронных сетей. Также для диагностирования нарушения безопасности может использоваться онтологический подход [4].

Применение искусственных нейронных сетей для диагностирования нарушений безопасности информации в инфокоммуникационных системах позволит повысить эффективность защиты от компьютерных атак в первую очередь за счет повышения достоверности диагностирования нарушений, и, соответственно, обоснованности принимаемых решений на реагирование. Помимо этого, можно говорить и о повышении оперативности диагностирования, поскольку, пройдя хоть и длительный процесс обучения, нейронная сеть способна в автоматическом режиме и в близком к реальному масштабе времени идентифицировать характеристики нарушений безопасности.

Следует отметить, что накопленные в результате диагностирования нарушений данные о компьютерных атаках могут быть использованы для корректировки (уточнения) уже созданных правил обнаружения атак или формирования новых. Реализация процедуры корректировки или создания новых правил обнаружения атак в реальном масштабе времени в автоматическом режиме позволяет строить адаптивные системы защиты информации, в том числе и на основе концепции информационных образов [5].

Применение искусственных нейронных сетей в задаче диагностирования нарушений безопасности позволит существенно повысить значения показателей эффективности защиты информаци от компьютерных атак в инфокоммуникационных системах.

СПИСОК ЛИТЕРАТУРЫ

1. Паращук И.Б. Сетевой мониторинг как ключевой этап подготовки и принятия решения по управлению информационной безопасностью региональных телекоммуникационных сетей // Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2015. С. 130-132.

2. Овсянников С.Н., Хмелевской В.П. Организация информационного процесса в системе автоматизации управления связью. Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 389-391.
3. Гришин А.В. Нейросетевые технологии в задачах обнаружения компьютерных атак. // Информационные технологии и вычислительные системы. 2011. № 1. С. 53-64.
4. Брунилин А.А., Бирюков М.А., Саенко И.Б. Модель и метод использования онтологий для управления разграничением доступа в едином информационном пространстве // Математические методы в технике и технологиях – ММТТ. 2016. № 6 (88). С. 122-124.
5. Авраменко В.С. Адаптивный контроль защищенности информации от несанкционированного доступа // Информация и космос. 2010. № 3. С. 116-119.

УДК: 004.056.5

ПРОГНОЗИРОВАНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Авраменко Владимир Семенович, Беденков Виктор Николаевич, Селяков Максим Николаевич
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: vsavr@yandex.ru, reanimatormail@gmail.com, maxolga801@mail.ru

Аннотация. Рассматривается проблема прогнозирования защищенности информации в автоматизированных системах. Представлены основные термины и определения, классификация прогнозов и методов прогнозирования защищенности информации.

Ключевые слова: *автоматизированная система; угроза; прогнозирование защищенности; метод прогнозирования.*

PREDICTING THE PROTECTION OF INFORMATION IN AUTOMATED SYSTEMS

Avramenko Vladimir, Bedenkov Viktor, Selyakov Maxim
Military academy of communications named after Marshal of the Soviet Union S. M. Budenny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: vsavr@yandex.ru, reanimatormail@gmail.com, maxolga801@mail.ru, t.+78122479437

Abstract. The paper deals with the problem of predicting the security of information in automated systems. The main terms and determination, classification of forecasts and forecasting methods of security of information are provided.

Keywords: *automated system; threat; security prediction; forecasting method.*

Автоматизированные системы (АС) в настоящее время активно развиваются и используются практически во всех сферах человеческой деятельности. Одной из ключевых проблем обеспечения эффективного функционирования АС является проблема защиты информации от несанкционированного доступа и компьютерных атак. Несмотря на постоянное совершенствование и развитие технологий и средств защиты информации (сканеров уязвимостей, систем обнаружения вторжений, атак, SIEM-систем и др.) по-прежнему наблюдается несоответствие возможностей систем защиты информации (СЗИ) в АС потенциалу средств и технологий кибератак.

Основным факторам, определяющим высокую сложность решения задачи эффективной защиты информации в современных АС, являются условия неопределенности функционирования АС, обусловленные противоречивостью и неполнотой информации о состоянии защищенности АС, и в первую очередь – об угрозах безопасности информации.

Одним из путей решения проблемы адекватности и инерционности реагирования на изменение состояния системы защиты информации в АС и условий ее функционирования (и в первую очередь – на новые угрозы безопасности) является реализации функции прогнозирования защищенности информации. Анализ существующих АС показал, что функция прогнозирования защищенности не реализуется в полной мере, отсутствуют эффективные технологии и средства прогнозирования отдельных угроз безопасности, уровня потенциальной опасности атакующей стороны, уровня защищенности информации в АС в целом. Одной из причин проблемы прогнозирования защищенности информации в АСН является недостаточная проработанность теоретических и методологических основ прогнозирования защищенности информации в АС.

В общем случае под защищённостью информации в АС понимается свойство противостоять созданию и реализации угроз безопасности информации. В теории управления функция прогнозирования рассматривается, как самостоятельная либо выделяется в качестве этапа реализации других управленческих функций. Также прогнозирование защищенности может выполняться в рамках задачи мониторинга защищённости [1]. В терминах теории эффективности задача прогнозирования состояния защищенности информации на определенный период времени может быть сформулирована как задача оценки потенциальной защищенности информации.

Основной целью прогнозирования защищенности является обеспечение запаса времени, достаточного для проведения мероприятий упреждающего характера на возможное нарушение

защищенного состояния АС, в первую очередь – на возможные реализации угроз безопасности защищаемых ресурсов.

При прогнозировании защищенности в качестве прогнозной величины могут использоваться такие характеристики защищенности как тип угрозы, количество и интенсивность появления уязвимостей (угроз, атак), величина потенциального ущерба и т.д. А для поддержки принятия решений по защите информации в АС в целом целесообразно использовать комплексные показатели защищенности, учитывающие как процессы нарушения безопасности, так и процессы контроля и восстановления защищенного состояния [2, 3].

По цели прогнозирования прогнозы защищенности могут быть поисковые и нормативные.

По временному охвату (горизонту прогнозирования, периоду упреждения) можно условно выделить долгосрочные, среднесрочные, краткосрочные и оперативные прогнозы защищенности. По времени осуществления прогнозы защищенности подразделяются на прогнозы в реальном масштабе времени и этапные прогнозы.

По способу представления результатов прогнозы защищенности информации могут быть точечными и интервальными.

Методы прогнозирования защищенности определяется задачами защиты информации, степенью неопределенности имеющейся информации о состоянии защищенности, условиями функционирования АС, требованиями к параметрам прогнозов. По характеру информации, на базе которой составляется прогноз защищенности, можно выделить фактографические, экспертные и комбинированные методы. При наличии статистических данных для прогнозирования защищенности целесообразно в первую очередь использовать методы, основанные на анализе динамических рядов характеристик (параметров) защищенности информации, в частности, методы экстраполяции. Для прогнозирования защищенности могут использоваться опережающие методы, основанные на использовании свойства научно-технической информации опережать реализацию научно-технических достижений. Среди методов этой группы для прогнозирования защищённости наиболее применим метод анализа публикаций и других источников информации о разрабатываемых и перспективных технологиях и средствах автоматизации, защиты информации, а также анализ сведений из неофициальных источников об уязвимостях, атаках и т.д.

Эффективность прогнозирования защищенности в основном определятся качеством прогнозов. Также при оценке эффективности прогнозирования необходимо учитывать оперативность и ресурсоемкость прогнозирования. На качество прогноза влияют выбранные методы прогнозирования, а также данные из источников, которые должны быть достоверны, сопоставимы, достаточно представительны, однородны и устойчивы. Такими источниками могут быть различного рода сенсоры системы защиты информации в АС, информация об уязвимостях и компьютерных атаках, поступающая как из открытых, так и из собственных источников, заключения экспертов.

Для оценки качества прогноза защищенности может использоваться такая величина как ошибка прогноза. Под ошибкой прогноза защищенности информации в АС понимается апостериорная величина отклонения прогноза от действительного состояния защищенности АС (разница между прогнозным и фактическим значениями).

Задачу прогнозирования состояния защищенности необходимо решать на всех стадиях жизненного цикла СЗИ в АС. На стадии проектирования в основном разрабатываются долгосрочные прогнозы. На стадии функционирования неопределенность и высокая динамика реализации большинства угроз требует выработки управляющих воздействий на систему защиты в минимальные сроки. Также прогнозирование необходимо при планировании внесения существенных изменений в защищаемую систему, в том числе и перед принятием решения на изменение ключевых элементов системы защиты информации, например, при масштабной реорганизации системы разграничения доступа в [4]. Перспективным является реализация функции прогнозного контроля защищенности информации на основе информационных образов элементов защищаемой системы [5].

Разработка и внедрение средств технологий автоматизированного прогнозирования защищенности в АС, функционирующих в условиях высокой степени неопределенности информации состояния защиты, позволит обеспечить возможность своевременного реагирования на новые угрозы безопасности, существенно повысить уровень защищённости информации в АС в целом.

СПИСОК ЛИТЕРАТУРЫ:

1. Паращук И.Б. Мониторинг безопасности информации в приложении к задачам управления качеством инфотелекоммуникационных сетей // Информация и космос. 2014. № 1. С. 57-59.
2. Козленко А.В., Авраменко В.С., Саенко И.Б., Кий А.В. Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности // Труды СПИИРАН. 2012. № 2 (21). С. 41-55.
3. Бушуев С.Н., Авраменко В.С., Козленко А.В. Оценка защищённости информации от несанкционированного доступа в условиях стохастической неопределенности угроз // Вопросы радиоэлектроники. 2013. Т.3. №1. С.82-85.
4. Саенко И.Б., Бирюков М.А. Методика интеграции локальных схем разграничения доступа к разнородным ресурсам единого информационного пространства // Информационные технологии в управлении (ИТУ-2016) Материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В.Г. Пешехонов. 2016. С. 758-762. Авраменко В.С.
5. Адаптивный контроль защищенности информации от несанкционированного доступа на основе информационных образов // Проблемы информационной безопасности. Компьютерные системы. 2010. № 2. С. 45-49.

УДК 004.056.5

ОЦЕНКА РИСКОВ СЕТЕВОЙ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ НЕЧЕТКОГО ЛОГИЧЕСКОГО ВЫВОДА

Агеев Сергей Александрович[1],Саенко Игорь Борисович[2]
[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mails: serg123_61@mail.ru, ibsaen@mail.ru

Аннотация. Представлены результаты синтеза и исследований адаптивных методов и алгоритмов обнаружения аномалий трафика и алгоритмов оперативной оценки рисков угроз сетевой и информационной безопасности мультисервисных сетей связи, основанных на методах нечеткого продукционного логического вывода. Основной идеей предложенного подходаявляется модификация и совместное применение методов безыдентификационных алгоритмов адаптации и методов, основанных на правилах нечеткого логического вывода, а также комбинация метода субтрактивной кластеризациии методов нечеткого продукционного вывода. Анализ экспериментальных результатов показал, что достигнутые результаты близки к потенциально достижимым.

Ключевые слова: *псевдоградиентный алгоритм; нечеткий логический вывод; субтрактивная кластеризация; система обнаружения и предупреждения вторжений; мультисервисная сеть связи.*

ASSESSMENT OF NETWORK COMPUTER SECURITY RISKS ON BASIS OF THE FUZZY LOGICAL INFERENCE

Ageev Sergey[1], Saenko Igor [2]
[1]Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
[2] St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
e-mails: serg123_61@mail.ru, ibsaen@mail.ru

Abstract. The paper presents resultes of synthesis and researches of the adaptive methods and algorithms of traffic anomalies detection and algorithms of operational threats risks assessment of network and information security for the multiservice communication networks based on methods of a fuzzy production logical inference. The main idea of the offered approach is a modification and combined use of methods of unidentification algorithms of adaptation and the methods based on rules of a fuzzy logical inference and also a combination of a method of a subtractive clustering and methods of a fuzzy production inference. The analysis of the experimental results showed that the achieved results are close to potentially achievable ones.

Keywords: *pseudo-graded algorithm; fuzzy logical inference; subtractive clustering; intrusion detection and warning system; multiservice communication network.*

При создании и эксплуатации мультисервисных сетей связи (МСС) важнейшей является проблема обеспечения ее безопасного функционирования и обеспечения безопасности циркулирующей в ней информации. Для решения данной проблемы необходимо применение методов, которые позволяют оперативно оценивать риски информационных угроз с заданной степенью достоверности [1].

При эксплуатации МСС одними из критериев ее нормального функционирования является нормальное поведение сетевого трафика и допустимый уровень рисков реализации угроз сетевой безопасности. В МСС присутствует весьма разнородный трафик [2], например, разнообразный мультимедийный трафик, который весьма чувствителен к задержкам, трафик передачи данных, трафик передачи управляющей информации, трафик электронной почты и т.д. При этом должны выполняться заданные требования к качеству предоставляемых услуг и сервисов.

Сложность информационно-логической и физической архитектур МСС, гетерогенность МСС, необходимость анализа большого количества различных сетевых и информационных параметров обуславливают объективные трудности в построении подсистем управления сетью и защиты сетевой и абонентской информации. Тем не менее, оперативное обнаружение аномалий сетевого состояния является одной из ключевых задач сетевого управления МСС.

Необходимо отметить, что особенностью МСС является высоко сегментированная топология, наличие нескольких точек сопряжения с другими сетями. Общий трафик системы уже нельзя контролировать из одной точки сети. Это обстоятельство обуславливает необходимость применения технологии интеллектуальных агентов (ИА) для решения подобного рода задач [2, 3].

С помощью ИА часть управленческих решений вырабатываются и реализуются сами на основе результатов оценки аномалий трафика и оценивания рисков сетевой и информационной безопасности. Подобный подход позволяет повысить оперативность принятия решений по противодействию каких-либо деструктивных воздействий на сеть, снизить служебный трафик управления. Вместе с тем, применение технологии ИА диктует необходимость применения устойчивых к изменению в широких пределах параметров трафика и простых в реализации алгоритмов обнаружения его аномалий, функционирующих в режиме времени, близком к реальному, а также эффективных алгоритмов оценки уровня рисков угроз сетевой и информационной безопасности. Решение данной задачи осложняется тем, что статистические свойства трафика МСС весьма различны как для различных условий эксплуатации МСС, так и для различных приложений, которые используют сервис, предоставляемый МСС.

Для экспериментальной проверки предложенных методов и алгоритмов был собран экспериментальный стенд. В работе проводилось генерирование как стационарного, так и нестационарного трафика, имеющего распределение Пуассона. Генерировалась атака типа «один-к-одному». Нестационарные процессы моделировались как мультипликативные случайные последовательности (СП) с различными модулирующими функциями – детерминированными и случайными. Случайные модулирующие функции представляли собой случайные процессы авторегрессии первого порядка с различными коэффициетами корреляции. Самоподобные трафики генерировались с помощью случайных процессов, имеющих ограниченное распределение Парето.

Полученные данные показывают, что время переходных процессов составляют несколько десятков отсчетов СП. Математическое ожидание модуля относительной ошибки оценивания предложенных алгоритмов составило не более 3–8% от абсолютного значения оцениваемой интенсивности СП. Подобные значения средних относительных ошибок для систем реального времени является приемлемой величиной. Размер скользящего окна для оценки характеристик трафика может быть выбран от 30 до 120 отсчетов.

Проведенные численные исследования алгоритма субтрактивной кластеризации показали его высокую устойчивость к различным изменениям параметров распределения признаков. Результаты анализа полученных экспериментальных данных показали, что области проекций значений признаков на координатные оси перекрываются для различных кластеров. Тем не менее, производится верное определение числа кластеров.

Иными словами, если центр кластера находится в достаточной близости от центра кластера известной угрозы, то считается, что риск идентифицирован с определенным значением коэффициента ранжирования. Если центр кластера находится на большом расстоянии от центров известных угроз, то независимо от того, в какой области он находится, риск считается максимальным, так как характеристики угрозы не определены. Далее полученные данные поступают на вход системы поддержки принятия решений.

Заключение. Анализ полученных результатов экспериментального моделирования позволяет сделать вывод о том, что предложенные алгоритмы могут быть реализованы в виде встраиваемых программно-аппаратных средств, функционирующих в режиме времени, близкому к реальному, и с качеством, близким к потенциально достижимому. Обучение предложенных алгоритмов целесообразно осуществлять на тестовых трафиковых трассах в период проектирования и модернизации МСС. Рассмотренный подход позволяет обеспечивать значения основных целевых функций сетевого и прикладного уровней МСС в части оценки и управления рисками информационной безопасности в области Парето-оптимальных значений.

В условиях динамично изменяющихся внешних условий и воздействий на МСС возможных деструктивных факторов данный подход является достаточным условием успешного ее функционирования.

Предложенная математическая модель оценки рисков информационной безопасности элементов МСС достаточно просто реализуется в виде встраиваемых программных средств как на языках высокого уровня, так на средствах программирования микроконтроллеров, сигнальных процессоров или программируемых логических интегральных схем.

Большинство решений по оценке рисков информационной безопасности элементов МСС подобное программное средство может принимать самостоятельно, что позволяет повысить оперативность выработки управленческих решений, а также снизить объем передаваемого технологического трафика в сети.

Работа выполнена при финансовой поддержке РФФИ (проект 15-07-07451) и при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007.

СПИСОК ЛИТЕРАТУРЫ

1. Агеев С.А., Бушуев А.С., Егоров Ю.П., Саенко И.Б. Концепция автоматизации управления информационной безопасностью в защищенных мультисервисных сетях специального назначения // Автоматизация процессов управления, №1, 2011. – С.50–57.

2. Саенко И.Б., Агеев С.А., Шерстюк Ю.М., Полубелова О.В. Концептуальные основы автоматизации управления защищенными мультисервисными сетями // Проблемы информационной безопасности. Компьютерные системы. №3, 2011. – С.30–39.
3. Гребешков А. Ю. Стандарты и технологии управления сетями связи. – М.: Эко-Трендз, 2003. – 288 с.

УДК 621.39

СРЕДСТВА И СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Алашеев Вадим Викторович, Латушко Николай Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: alvdmv@mail.ru

Аннотация. Рассмотрены способы и средства защиты информационных ресурсов должностных лиц на объектах информатизации от возможности несанкционированного доступа и перехвата информации ограниченного распространения с помощью разведывательных технических средств, и систем добывания информации, скрытно устанавливаемых на объектах информатизации, где циркулирует конфиденциальная информация.

Ключевые слова: *способы; средства; объект информатизации; конфиденциальная информация; обнаружения.*

MEANS AND METHODS OF PROTECTION OF INFORMATION RESOURCES

Alasheev Vadim, Latushko Nikolay
Military Academy of communications (St. Petersburg)
Russia, St. Petersburg, Tikhoretskiy pr., 3
e-mail: alvdmv@mail.ru

Abstract. The paper examines the ways and means of protection of information resources officers on the objects of information from the possibility of unauthorized access and interception of restricted information with the intelligence technical means and systems of obtaining information clandestinely installed on objects of information, where circulating confidential information

Keywords: *ways; means; object information; confidential information; detection.*

С внедрением современных информационно-телекоммуникационных технологий в сферы деятельности должностных лиц (ДЛ) объектов информатизации значительно возросли возможности несанкционированного доступа и перехвата информации ограниченного распространения с помощью разведывательных технических средств и систем добывания информации, скрытно устанавливаемых на объектах информатизации (ОИ), где циркулирует конфиденциальная информация. Ввиду того, что способы внедрения таких средств непрерывно совершенствуются, необходим поиск путей, позволяющих своевременно обнаруживать, идентифицировать и нейтрализовать технические каналы утечки информации как естественного, так и искусственного происхождения на объектах ОИ [1].

Решение таких задач возможно при кардинальном изменении существующего подхода к процессу контролю защищенности информации, а также путем решения частных задач по разработке новых алгоритмов обнаружения, идентификации, локализации технических каналов утечки информации (ТКУИ), определению межконтрольных сроков и планированию контроля.

Необходимость обеспечения эффективной защиты информации (ЗИ) на ОИ в различных условиях динамично меняющейся обстановки от подразделений службы безопасности требует кроме планового и периодического контроля защищенности информации и оперативную оценку защищенности информации на объекте информатизации.

Одно из важнейших направлений защиты информации является контроль защищенности информации от ее утечки по ТКУИ на ОИ, целью которого является выявление потенциальных естественных и искусственных, созданных с помощью специальных технических средств (СТС) ТКУИ [1].

Способ по обнаружению несанкционированно установленных на ОИ специальных электронных устройств

Предлагается к рассмотрению алгоритм обнаружения несанкционированно установленных на ОИ специальных электронных устройств, который обеспечивает повышение вероятности их обнаружения за счет разработки системы обнаружения СТС [2]. Предлагаемая система обнаружения СТС состоит из:

1 – контролируемого помещения;
2 – контролируемой зоны;
3 – тестового специального технического средства;
4 – приемника;
5 – передатчика;

6 – узконаправленной передающей антенны;

7 – узконаправленной приемной антенны;

8 – ПЭВМ со специальным программным обеспечением, формирующей тестовую последовательность и сигнал об обнаружении специальных технических средств.

Данный способ обеспечивает более высокую вероятность их обнаружения, при отсутствии предварительных данных о параметрах электромагнитных сигналов радиоэлектронных средств, которые установлены в пределах контролируемой зоны.

Способ по идентификации многопараметрических объектов

Возможность повышения вероятности идентификации разнородных СТС обеспечивается путём использования механизмов анализа, позволяющих выявлять незначительные изменения нескольких контролируемых параметров идентифицируемых СТС и возможности при этом их достоверной идентификации [3].

Благодаря использованию в разработанном алгоритме теории распознавания образов и алгоритмов автоматической иерархической классификации обеспечивается повышение вероятности идентификации СТС, снимается неопределенность относительно типа, подкласса, класса идентифицируемого СТС при его идентификации за счет учета: новых введенных показателей: центров тяжести параметров классов, подклассов СТС, использования механизмов нормировки и поэтапного сравнения центров тяжести параметров классов, подклассов эталонных и идентифицируемого СТС, которые позволяют выявлять с высокой вероятностью принадлежность идентифицируемого СТС соответственно к классу, подклассу и типу.

Способ динамического обнаружения малогабаритных скрытых средств, способствующих утечке информации, несанкционированно установленных на подвижном объекте

Способ относится к средствам контроля работы электронного оборудования и может быть использовано для выявления и устранения ТКУИ, образованных с помощью несанкционированно установленных на подвижном объекте скрытых средств (НУОСС), способствующих утечке информации, например, скрытых радиомикрофонов и видеокамер [4].

При использовании предложенного способа для обнаружения НУОСС, способствующих утечке информации, снижается количество ложных обнаружений других радиоэлектронных средств, не являющихся НУОСС, способствующих утечке информации и расположенных за пределами подвижного объекта, и поэтому повышается достоверность обнаружения несанкционированно установленных на подвижном объекте скрытых средств, способствующих утечке информации.

Достоинством способа является, повышение достоверности обнаружения несанкционированно установленных устройств и расширении области применения.

Способ определения местоположения несанкционированно установленных на объекте электронных устройств/ Целью является разработка способа обнаружения несанкционированно установленных в этой зоне радиоэлектронных устройств (НУОЭУ), обеспечивающих повышение точности определения местоположения НУОЭУ при отсутствии предварительных данных о параметрах электромагнитных сигналов радиоэлектронных средств, в том числе установленных в пределах контролируемой зоны (КЗ) [5].

Предлагаемый способ реализуется следующим образом. В пределах контролируемой зоны установлен высокочастотный радиопередатчик с подключенной узконаправленной передающей антенной, расположенной на поворотном устройстве, сканирующий радиоприемник с подключенной ненаправленной (штыревой) приемной антенной. В пределах контролируемой зоны могут быть обнаружены электромагнитные сигналы от НУОЭУ и источников электромагнитного излучения (ИЭМИ), расположенных за пределами контролируемой зоны.

Средством защиты является устройство или алгоритм, доведенный до программной реализации, который незначительно, но обязательно снижает качество функционирования объекта защиты в интересах легитимного пользователя и принципиально, либо полностью, затрудняет его использование в интересах нелегитимного пользователя.

Наиболее часто реализуется вариант, при котором взаимодействие организуется и обеспечивается между объектами различных категорий. При этом преобладающая часть известных средств защиты предназначена для применения на однородных объектах, что вызывает необходимость разработки соответствующих способов защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Стародубцев Ю.И. Управление качеством информационных услуг / Ю.И. Стародубцев, А.Н. Бегаев, М.А. Давлятова; под общ. Ред. Ю.И. Стародубцева. – СПб. : Изд-во Политехн. Ун-та, 2017. – 454 с.
2. Алашеев В.В., Стародубцев П.Ю. и др. Способ обнаружения несанкционированно установленных на объекте специальных электронных устройств. Патент РФ № 2397501 от 23.03.2009 г.
3. Алашеев В.В., Стародубцев Ю.И. и др. Способ идентификации многопараметрических объектов. Патент РФ № 2395817 от 27.07.2010 г.
4. Гречишников Е.В. и др. Способ динамического обнаружения малогабаритных скрытых средств, способствующих утечке информации, несанкционированно установленных на подвижном объекте. Патент РФ № 2503023 от 27.12.2013 г.
5. Стародубцев Ю.И., Сухорукова Е.В. и др. Способ определения местоположения несанкционированно установленных на объекте электронных устройств. Патент РФ № 2558333 от 27.07.2015 г.

УДК 681.51

РАЗВЕРТЫВАНИЕ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ ДИСТАНЦИОННОГО ОБУЧЕНИЯ В СУЩЕСТВУЮЩЕЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ

Алексеев Олег Владимирович, Ногин Сергей Борисович, Чесноков Александр Валерьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: piramida-17@mail.ru

Аннотация. В докладе рассматривается развертывание в функционирующей системе управления с жестко заданной структурой и жестко заданным программным обеспечением виртуальной инфраструктуры (один или несколько серверов приложений, ряд виртуальных машин, внутреннюю виртуальную сеть) для обеспечения подготовки пользователей.

Ключевые слова: *виртуальная инфраструктура; среда виртуализации; подготовка пользователей.*

DEPLOYMENT OF VIRTUAL INFRASTRUCTURE REMOTE TRAINING IN THE EXISTING AUTOMATED CONTROL SYSTEM

Alekseev Oleg, Nogin Sergei, Chesnokov Alexander
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretskiy pr., 3
e-mail: piramida-17@mail.ru

Abstract. The report examines the deployment in a functioning management system with a rigidly defined structure and hard-coded virtual infrastructure software (one or more several application servers, a number of virtual machines, an internal virtual network) to provide user training.

Keywords: *virtual infrastructure; virtualization environment; user training.*

В функционирующей системе управления предлагается внедрить инфраструктуру облачных вычислений, предназначенную для обучения (подготовки) пользователей.

При разработке механизма внедрения виртуальной инфраструктуры необходимо оценить пропускную способность существующей системы управления и ее потенциальные узкие места.

Основным узким местом при увеличении плотности виртуальных машин является объем памяти; однако сейчас появилось множество серверов, с намного большим объемом памяти, что устраняет это узкое место.

Облачные вычисления нивелируют это узкое место, устраняя проблему плотности машин – ее решение становится ответственностью поставщика облака, что освобождает пользователей облака от необходимости заботиться об этом.

В качестве среды виртуализации будет использоваться платформа для организации управления облачной инфраструктурой и виртуальными окружениями Open Nebula, что определяется программным обеспечением функционирующей системой управления.

Предлагается следующий алгоритм развертывания виртуальной инфраструктуры:

1. Определение требуемых вычислительных ресурсов.

1.1. Если в существующей системе функционирует интеграционный комплекс информационных сервисов (ИКИС), то платформу OpenNebulaразворачиваем в кластере серверов приложений.

1.2. Если ИКИС не развернут, то платформа виртуализации устанавливается в наименее нагруженный домен.

1.2.1. Если число доменов до 10, то платформаOpenNebulaразворачиваетсяв корневом домене на сервере функциональной группы (СФГ) (домен верхнего уровня).

1.2.2. Если число доменов больше 10, то платформа разворачивается в домене с наименьшимколичеством пользователей (основной показатель) и наибольшим свободным местом на диске на СФГ (второй показатель).

2. Развертывание платформыOpenNebula на сервере выбранного домена. Установку и настройку программного обеспечения платформы осуществляет администратор сети (так как сервер уже существует, никаких других сетевых настроек осуществлять не надо).

3. Настройка доступа к платформе OpenNebula. Настройку осуществляетадминистратор безопасности.

В справочнике абонентов и ресурсов(САИР) создаются пользователи для работы с OpenNebula.

В САИР как ресурс прописывается доступ к программам OpenNebula для данных пользователей.

4. Выделяется дисковое пространство для хранения образов виртуальных структур. Если функционирует ИКИС, то пространство выделяется в кластере хранения. Если ИКИС не функционирует, то пространство выделяется на том же СФГ, где развернуто программное

обеспечение платформы OpenNebula. Расчет дискового пространства производится исходя из параметров: виртуальная машина – 5 Гб (в виртуальной машине создается динамический диск). СФГ – 10 Гб; виртуальный домен – 100 Гб – цифры взяты исходя из практической реализации виртуальных структур. Общий объем дискового пространства исходя их 2-3 доменов, 1 СФГ, 1 вычислительный комплекс, 1 автоматизированное рабочее место.

5. Резервированиефизического дискового пространства для развертывания виртуальных структур.
6. Создание на виртуальных машинах типовых АРМ должностных лиц.
7. Создание виртуальной локальной сети в рамках одного домена.
8. Создание виртуального домена (на базе сервера функциональной группы).
9. Резервирование вOpenNebula дискового пространства для запуска виртуальных структур из расчета создаваемой виртуальной структуры. Реальное физическое пространство для запуска может быть выбрано на любом сервере или хранилище, где есть место. На период проведения мероприятийвыделенное дисковое пространство будет задействовано с использованием механизмов платформы OpenNebula.

СПИСОК ЛИТЕРАТУРЫ

1. Спрос на устройства хранения в мире взаимосвязанных данных. // Seagate and BlackArmor, 2015. // [Электронный ресурс]: http://www.seagate.com/ru/ru/tech-insights/demand-for-storage.html.
2. Новые информационные и сетевые технологии в системах управления военного назначения. Часть1. Новые сетевые технологии в системах управления военного назначения. Учебник / Под редакцией С.М. Одоевского. СПб.: ВАС, 2010 – 432 с.
3. Новые информационные и сетевые технологии в системах управления военного назначения. Часть 2. Новые сетевые технологии в системах управления военного назначения. Учебник / Под редакцией И.Б. Саенко. СПб.: ВАС, 2010 – 520 с.

УДК 681.51

ВНЕДРЕНИЕ СЕРВИСА «ИНФРАСТРУКТУРА КАК СЕРВИС» ДЛЯ ПРОВЕДЕНИЯ КОМПЛЕКСНЫХ ПРАКТИЧЕСКИХ ЗАНЯТИЙ С ДОЛЖНОСТНЫМИ ЛИЦАМИ ОРГАНА УПРАВЛЕНИЯ

Алексеев Олег Владимирович, Ногин Сергей Борисович, Чесноков Александр Валерьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: piramida-17@mail.ru

Аннотация. В докладе рассматривается механизм использования сервиса «IaaS» в функционирующей системе управления с жестко заданной структурой и жестко заданным программным обеспечением виртуальной инфраструктуры для обеспечения подготовки пользователей.

Ключевые слова: *виртуальная инфраструктура; среда виртуализации; инфраструктура как сервис; подготовка пользователей.*

IMPLEMENTATION OF «INFRASTRUCTURE AS SERVICE» SERVICE FOR CONDUCTING INTEGRATED PRACTICAL LESSONS WITH OFFICERS OF THE GOVERNING BODY

Alekseev Oleg, Nogin Sergei, Chesnokov Alexander
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretskiy pr., 3
e-mail: piramida-17@mail.ru

Abstract. The report discusses the mechanism for using the service «IaaS» in a functioning management system with a rigidly defined structure and hard-coded virtual infrastructure software to provide user training

Keywords: *virtual infrastructure; virtualization environment; infrastructure as service; user training.*

В функционирующей системе управления предлагается развернуть виртуальную инфраструктуру (серверы функциональной группы, виртуальных машин автоматизированных рабочих мест, внутреннюю виртуальную локальную сеть), предназначенную для обучения (подготовки) пользователей.

В качестве среды виртуализации с учетом имеющегося в системе программного обеспечения использовать среду виртуализации Open Nebula.

Имеются ограничения:

1. Существующая логическая, в связке с технической, структура стационарной части системы управления (корневой домен (домен первого уровня), домены управлений (отделов).

2. Жестко зафиксированное программное обеспечениеавтоматизированных рабочих мест (АРМ) должностных лиц (ДЛ).

Для проведения практических занятий с должностными лицами на существующих технических средствах (в том числе АРМ ДЛ) развертывается виртуальная инфраструктура, повторяющая структуру функционирующей системы управления. Пользователям предоставляется доступ со своих физических АРМ к виртуальной инфраструктуре для отработки соответствующих заданий.

Предложения по внедрению сервиса «IaaS» в существующую систему управления:

1. Создать виртуальную инфраструктуру, соответствующую системе управления с использованием платформы для организации управленияcloud-инфраструктурой и виртуальными окружениями OpenNebula:

1.1. Создать образы виртуальных машин: сервера функциональной группы, АРМ, виртуального маршрутизатора. В качестве вычислительного комплекса (ВК) виртуальной инфраструктуры используется функционирующий ВК действующей автоматизированной системы.

1.2. Создать из подготовленных образов инфраструктуру соответствующей системы управления (необходимое количество доменов и соответствующее количество АРМ ДЛ).

1.3. Настроить виртуальную локальную сеть (задать IP- адреса, имена компьютеров, правила маршрутизации и др.).

1.4. Создать виртуальные домены.

1.5. Настроить справочник абонентов и ресурсов САИР для каждого созданного домена (включая домен верхнего уровня).

2. Сохранить виртуальную инфраструктуру средствами платформы OpenNebula в соответствующем хранилище.

3. Зарегистрировать созданную инфраструктуру в САИР.

4. Создать в САИР действующей системы управления пользователя с правами администратора сети для созданнойинфраструктуры.

5. Создать в САИР действующей системы пользователя с правами администратора безопасности для созданной инфраструктуры.

6. Настроить точку входа (удаленный доступ) в созданную инфраструктуру для администратора сети и администратора безопасности.

7. Настроить точку входа для пользователей для созданной инфраструктуры (удаленный доступ для пользователей).

8. Создать в OpenNebula скрипт для развертывания виртуальнойинфраструктуры.

При подготовке к проведению практических занятий с должностными лицами администратор безопасности действующей автоматизированной системы управления осуществляет развертывание созданной виртуальной инфраструктуры и ее изменение (при необходимости) (изменение количества доменов, рабочих мест и другое) исходя из целей проводимых занятий и выдает данные соответствующих учетных записей пользователям.

В период проведения занятий должностные лица органа управления входят со своих физических рабочих мест через заданные точки входа с использованием данных полученных учетных записей в виртуальную инфраструктуру, где и отрабатывают соответствующие задания.

СПИСОК ЛИТЕРАТУРЫ

1. Спрос на устройства хранения в мире взаимосвязанных данных. // Seagate and BlackArmor, 2015. // [Электронный ресурс]: http://www.seagate.com/ru/ru/tech-insights/demand-for-storage.html.
2. Новые информационные и сетевые технологии в системах управления военного назначения. Часть1. Новые сетевые технологии в системах управления военного назначения. Учебник / Под редакцией С.М. Одоевского. СПб.: ВАС, 2010 – 432 с.
3. Новые информационные и сетевые технологии в системах управления военного назначения. Часть 2. Новые сетевые технологии в системах управления военного назначения. Учебник / Под редакцией И.Б. Саенко. СПб.: ВАС, 2010 – 520 с.

УДК 621.391(075.8)

ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ СВЯЗЬЮ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Башкирцев Андрей Сергеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: ab098@yandex.ru

Аннотация. Сформулированы общие требования к безопасности информационного обмена в автоматизированных системах управления связью специального назначения, а также предпринята попытка определения основных показателей, характеризующих безопасность информационного обмена в автоматизированных системах управления связью специального назначения

Ключевые слова: *ароматизированная система управления связью; информационный обмен; показатели качества; информационная безопасность.*

INDEXES OF SECURITY OF INFORMATION EXCHANGE IN AUTOMATED CONTROL SYSTEMS OF COMMUNICATION OF SPECIAL PURPOSE

Bashkirtsev Andrey
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: ab098@yandex.ru

Abstract. General requirements are formulated for the security of information exchange in automated communication systems for special purposes, and an attempt is also made to determine the main indicators characterizing the security of information exchange in automated communication systems for special purpose communications

Keywords: *automatized communication control system; information exchange; quality indicators; information security.*

Одной из основных компонент любой системы связи (СС) специального назначения (СН), обеспечивающей ее эффективное функционирование, является ее система управления, которая, как правило, являясь автоматизированной представляет собой организационно-техническое объединение сил и средств автоматизации и абонентских сетей передачи данных, развертываемых на пунктах управления связью и элемента х системы связи для обеспечения автоматизированного управления связью.

Таким образом, автоматизированные системы управления связью (АСУС) СН являясь ядром сети, обеспечивающем устойчивое и надежное функционирование СС СН и должна отвечать требованиям по устойчивости, непрерывности оперативности и скрытности процесса управления, который она реализует. Одной из ключевых составляющих, позволяющих обеспечить соответствие процесса автоматизированного управления связью этим требованиям является, обеспечение безопасности в АСУС СН [1].

Процесс обеспечения безопасности в АСУС СН общем случае направлен на реализацию возможностей по опознавания пользователей системы управления и соответствующих прикладных программ, что гарантирует конфиденциальность и целостность обмена информацией управления и предотвращает несанкционированный доступ к ней, а также сохранения целостности данных при их хранении и передачи по сети служебной связи АСУС СН и должен реализовываться подсистемой управления безопасностью АСУС СН.

Общие требования к подсистеме управления безопасностью АСУС СН с точки зрения обеспечения безопасности сводятся к применению сертифицированных программно-аппаратных средств в пунктах управления связью, криптографической защиты всей управляющей информации, организации контроля целостности информации, передаваемой по каналам сети служебной связи, к использованию стандартных протоколов управления, обеспечивающих информационную безопасность [2].

Исходя из вышеизложенного, можно сделать вывод, что при создании АСУС СН необходимо задавать требования к ее информационной безопасности, а управление потоками информации осуществлять на основе специальных алгоритмов и протоколов, гарантирующих безопасность процедур маршрутизации и обеспечивающих выполнение заданных требований по безопасности информационного обмена в АСУС СН.

Учитывая, что в общем случае под безопасность информационного обмена можно понимать способность системы служебной связи АСУС СН обеспечивать разведзащищенность и имитостойкость, которая достигается путем обеспечения сохранения в тайне от нарушителя содержания передаваемой информации и противостоянию ввода ложной информации, необходимо сформировать основные критерии оценки информационной безопасности, которые должны базироваться на соответствующей системе показателей качества информационной безопасности и прежде всего безопасности информационного обмена (СПК БИО).

Определения оптимальной СПК БИО заключается в выборе из некого множества сочетаний объема, номенклатуры и области допустимых значений параметров, характеризующих БИО, параметров с их конкретными значениями. Выбор множества параметров, характеризующих БИО можно осуществлять только на основе сравнения множества различных альтернатив.

Решения такой задачи заключается в построении адекватной модели СПК, характеризующей ИБ.

В общем случае модель СПК, характеризующей ИБ представляет собой вектор параметров безопасности ИО, который количественно характеризует разведзащищенность процесса информационного обмена и безопасность передачи информации управления и может быть описан с помощью двух параметров - среднего время вскрытия контура управления АСУС СН и коэффициента засекречивания информации управления.

Кроме этого параметром (показателем) безопасности передачи управляющей информации может служить коэффициент засекречивания информации управления, циркулирующей контуре

управления по каналам служебной связи и имеющий смысл обратный риску компрометации (рассекречивания) служебной информации.

Вероятность компрометации информации управления при ее прохождении через элементы АСУС СН зависит от соотношения числа засекреченных и незасекреченных каналов управления и сигнализации [3].

Частный критерий оценивания безопасности информационного обмена в АСУС СН может быть задан в виде совместной условной вероятности выполнения требований по разведзащищенности процесса информационного обмена и безопасности передачи информации управления по каналам служебной связи на каждом этапе управления в АСУС СН

Таким образом представлен обобщенный подход к синтезу показателей качества безопасности информационного обмена в АСУС СН, а также определены общие подходы к заданию вероятностного критерия оценивания безопасности информационного обмена в АСУС СН.

СПИСОК ЛИТЕРАТУРЫ

1. Перспективный облик автоматизированных систем управления связью силовых министерств и ведомств. Башкирцев А.С., Шинкарев С.А. Региональная информатика «РИ-2016» - юбилейная XV Санкт-Петербургская международная конференция – СПб 2016 г.
2. Автоматизированная система управления связью Вооруженных Сил Российской Федерации и приоритетные направления ее развития. Арсланов Х.А. Башкирцев А.С. Лихачев А.М. Информационно-телекоммуникационные технологии. Системы, средства связи и управления: Информационно-аналитический сборник / Под ред. С.В. Ионова; АО «Концерн «Созвездие». Воронеж, 2016. № 2. 278 с.
3. Вариант формулировки показателей качества современных средств доверенной загрузки и их роль при решении проблем безопасности алгоритмов управления инфотелекоммуникационными системами специального назначения. Вопросы оборонной техники. Серия 16: Башкирцев А.С. Паращук И.Б. Саяркин Л.А. Технические средства противодействия терроризму. Издательство: Научно-производственное объединение специальных материалов (Санкт-Петербург) ISSN: 2306-1456

УДК 681.5.015

ОРГАНИЗАЦИЯ РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ РАЗНОРОДНЫХ СРЕДСТВ АВТОМАТИЗАЦИИ

Башкирцев Андрей Сергеевич, Зибров Олег Павлович
Зобнин Константин Александрович, Усачёв Игорь Владимирович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: rus6283@list.ru

Аннотация. Рассмотрены вопросыобъединения нескольких АСУ на базе единого информационного пространства (ЕИП) и появления ряда необходимых условий их функционирования, таких как: задача комплексной защиты информации и задача разграничения доступа к ресурсам системы.

Ключевые слова: *автоматизированные системы управления; защита информации; разграничение доступа; единое информационное пространство.*

ORGANIZATION OF ACCES TO RESOURCES OF NETEROGENEOUS MEDIA AUTOMATION

Bashkirtcev Andrey, Zibrov Oleg, Zobnin Konstantin, Usachev Igor
Millitary Academy of Communications named S.M. Budyonnogo
Russia, St. Peterburg, Tikhoretsky pr., 3
e-mail: rus6283@list.ru

Abstract. The paper considers the issues combining multiple ACS on a single information space appearance some necessary conditions functioning, such as the complex task of information security and the challenge of differentiation access to system resources.

Keywords: *automated controlsystem; information security; access control; unified information space.*

Новейшие АСУ сочетают большой объем информационного наполнения с передовыми технологическими разработками. Постоянное техническое совершенствование увеличивает время разработки автоматизированных систем, не позволяют обеспечить глубокую интеграцию разнородных АСУ в единую АСУ на базе единого информационного пространства и приводят к нерациональным затратам на разработку средств информационно-технического сопряжения, которые с появлением каждой новой автоматизированной системы управления необходимо создавать заново.

Следует также отметить, что сопряжение различных АСУ, как правило, выполняется с большими временными затратами, отсутствием взаимной заинтересованности разработчиков этих автоматизированных систем в обеспечении их взаимодействия на необходимом для выполнения задач по предназначению уровне и другими, присущими работе такого рода сложностями. Кроме этого, модернизация программного обеспечения АСУ одной из сторон, ведущая к появлению новой версии

программного обеспечения, приводит к нарушению информационно-технического взаимодействия между ними.

Практика создания автоматизированных систем управления военного назначения также показала сложность решения задачи их увязки в единую автоматизированную систему управления Вооруженных Сил. Однако в ходе выполнения предприятиями ОПК работ по автоматизации управления ВооруженнымиСилами Российской Федерации, проведенными в последнее десятилетие получен научно-технический задел, который в перспективе позволяет создать АС СН, имеющие совместимое лингвистическое, программное и информационное обеспечение.

В таких условиях чрезвычайно важным является вопрос разграничения доступа к информационным ресурсам и недопущение угрозы нарушения конфиденциальности информации со стороны нарушителя (злоумышленника), вызванное намеренно или непреднамеренно, которое способно неблагоприятно повлиять на базы данных (БД), нарушая ее основные качественные характеристики (свойства).

В условиях повышенных требований к безопасности информации, находящейся в БД АС СН, возникает необходимость осуществления точных и корректных настроек схем разграничения доступа к БД АС СН, как на этапе их первоначального заведения, так и в процессе их ведения.

Таким образом, при объединении нескольких АСУ на базе единого информационного пространства (ЕИП) появляется ряд необходимых условий функционирования такой системы, а именно, задача комплексной защиты информации и задача разграничения доступа к ресурсам системы.

Таким образом достигается соблюдение трех основных требований: конфиденциальности, доступности и целостности данных. Стоит отметить, что под ресурсами системы понимаются как сама информация, так и вычислительные мощности системы.

При подобной организации администраторы безопасности вправе использовать различные модели разграничения доступа, отвечающие требованиям защиты информации от несанкционированного доступа (ЗИ от НСД).

Исходя из специфики решения задач средствами каждой конкретной АСУ модели доступа зачастую не совпадают. В АСУ может использоваться мандатная, ролевая, дискреционная или комбинированные модели доступа, которые при функционировании должны обеспечивать требуемый уровень ЗИ от НСД.

Анализ угроз безопасности информации в автоматизированных системах (АС) специального назначения (СН) показывает, что основным нарушителем и источником не преднамеренной угрозы является санкционированный пользователь.

Вероятный противник будет использовать эти нарушения в своих целях, осуществляя при этом преднамеренные и случайные угрозы безопасности информации в АС СН.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 51624–00. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. – М.: Изд–во стандартов, 2000.
2. Бочков М. В. Теоретические основы адаптивной защиты информации в вычислительных сетях от несанкционированного доступа: Монография. Под ред. Бушуева С. Н. и Комаровича В.Ф. – Орел: Академия Спецсвязи России, 2004 г. – 224 с.
3. Карпов Е.А., Буренин Н.И., Зюзин Н.А. Единое информационное пространство: проблемы создания. – Военная Мысль, 2004. – №8. – 47 с.

УДК621.391(075.8)

МЕЖСЕТЕВЫЕ ЭКРАНЫ КАК ЭЛЕМЕНТ АРХИТЕКТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИСИСТЕМ УПРАВЛЕНИЯ СОВРЕМЕННЫМИ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ И ЦЕНТРАМИ ОБРАБОТКИ ДАННЫХ

Башкирцев Андрей Сергеевич[1], Михайличенко Николай Валерьевич[1], Паращук Игорь Борисович[2]
[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mails: ab098@ya.ru, shchuk@rambler.ru, 23esn2008@rambler.ru

Аннотация. Проведен анализ достоинств, особенностей и перспектив применения межсетевых экранов в рамках архитектуры информационной безопасности систем управления современными телекоммуникационными сетями и центрами обработки данных. Проанализированы одноуровневые и многоуровневые межсетевые экраны, их функции и уровни применения для защиты каналов и элементов системы управления.

Ключевые слова: *межсетевой экран; система управления; телекоммуникационная сеть; центр обработки данных; информационная безопасность.*

FIREWALLS AN ELEMENT OFCONTROL SYSTEMS INFORMATION SECURITY ARCHITECTURE OF CONTEMPORARY TELECOMMUNICATION NETWORKS AND DATA CENTERS

Bashkirtsev Andrey [1], Mikhailichenko Nikolay [1],Parashchuk Igor [2]
[1]Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
[2] St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
e-mails: ab098@ya.ru, shchuk@rambler.ru, 23esn2008@rambler.ru

Abstract. The advantages, peculiarities and prospects of using firewalls within the framework of the information security architecture of control systems of modern telecommunication networks and data processing centers have been analyzed. Single-level and multi-level firewalls, their functions and application levels for protecting channels and control system elements are analyzed.

Keywords: *firewall; control system; telecommunication network; data center; information security.*

Известно, что типовая структура комплексной системы защиты информации (СЗИ), нацеленной на обеспечение безопасности систем управления (СУ) современными телекоммуникационными сетями (ТКС) и центрами обработки данных (ЦОД), включает ряд подсистем: доступа (подсистему защиты от несанкционированного доступа); обеспечения безопасной передачи информации; идентификации, аутентификации, регистрации и учета; защиты информации в базах данных; обеспечения безопасности операционных систем; антивирусной защиты; обнаружения компьютерных атак; криптографической защиты информации; подсистему защиты proxy-сервера и подсистему автоматизированного управления СЗИ.

При этом, по праву на первом месте стоит подсистема доступа (подсистема защиты от несанкционированного доступа), которая объединяет механизмы управления доступом и предназначена для предотвращения несанкционированного использования ресурсов СУ ТКС и ЦОД. Разработано множество средств для обеспечения защиты от несанкционированного доступа (НСД), предназначенных для использования на различных компьютерах СУ с разными операционными системами (ОС), но по-прежнему, несмотря на многолетнее использование, в качестве одного из главных направлений защиты эксперты отдают предпочтение межсетевым экранам (firewalls), призванным контролировать доступ к информации, циркулирующей по каналам СУ ТКС и ЦОД со стороны пользователей сети общего доступа (внешних сетей). Межсетевые экраны (брандмауэры, firewalls) занимают важное место в архитектуре безопасности СУ ТКС и ЦОД [1-3].

Они используются для защиты каналов и элементов СУ ТКС и ЦОД посредством контроля внешнего доступа к внутренним сетям предприятия и наоборот. Межсетевые экраны (МЭ) могут использоваться для создания «периметра безопасности», который обеспечивает защиту системы управления ТКС и ЦОД на сетевом уровне, позволяя таким образом упростить требования к защищенности отдельных компьютеров и рабочих мест СУ.

Концепция межсетевых экранов включает реализацию: политики безопасности, определяющей правила доступа к ресурсам и сервисам СУ ТКС и ЦОД и используемые для этого средства и протоколы; дополнительных механизмов аутентификации; фильтрацию пакетов; шлюзы для приложений, которые не позволяют эффективно применять фильтрацию пакетов, обычно реализуемые при помощи функций proxy-сервера.

В целом, задача межсетевого экранирования для процессов управления ТКС и ЦОД может быть сформулирована следующим образом. Пусть имеется две системы (СУ ТКС и ЦОД и Интернет) или два множества информационных систем. Экран – это средство разграничения доступа клиентов из одного множества систем к информации, хранящейся на серверах в другом множестве. Экран выполняет свои функции, контролируя все информационные потоки между этими двумя множествами систем, работая как некоторая «информационная мембрана». В этом смысле экран – набор фильтров, анализирующих проходящую через них информацию и, на основе заложенных в них алгоритмов, принимающих решение: пропустить ли эту информацию или отказать в ее пересылке. Кроме того, такая система может выполнять регистрацию событий, связанных с процессами разграничения доступа, в частности, фиксировать все «незаконные» попытки доступа к информации (командам) управления ТКС и ЦОД и, дополнительно, сигнализировать о ситуациях, требующих немедленной реакции, то есть поднимать тревогу.

Обычно экранирующие системы делают несимметричными. Для экранов определяются понятия «внутри» и «снаружи», и задача экрана состоит в защите внутренней системы – СУ ТКС и ЦОД от «потенциально враждебного» окружения. При этом важнейшим примером потенциально враждебной внешней сети обычно является глобальная сеть Интернет. Различают пять основных вариантов организации МЭ для СУ ТКС и ЦОД, ориентированных на уровень модели OSI, на котором производится фильтрация управляющего трафика. Поэтому можно говорить о четырех типах одноуровневых МЭ: экранирующих концентраторах (канальный уровень), экранирующих маршрутизаторах (сетевой уровень), транспортном экранировании (транспортный уровень), шлюзах

сеансового уровня (сеансовый уровень), прикладных экранах (прикладной уровень), и о том, что в настоящее время, наряду с одноуровневыми межсетевыми экранами, все большую популярность приобретают комплексные экраны, охватывающие уровни от сетевого до прикладного, поскольку подобные продукты соединяют в себе лучшие свойства одноуровневых экранов разных видов [3].

Несмотря на почтенный возраст использования, межсетевой экран до сих пор является наиболее распространенным средством усиления традиционных средств защиты СУ ТКС и ЦОД от несанкционированного доступа и активно применяется для обеспечения защиты данных при организации межсетевого взаимодействия. Конкретные реализации МЭ в значительной степени зависят от используемых вычислительных платформ, но, тем не менее, все системы этого класса используют два механизма, один из которых обеспечивает блокировку управляющего трафика (команд), а второй, наоборот, разрешает обмен данными для управления. При этом некоторые версии МЭ и методы экранирования делают упор на блокировании нежелательного трафика, а другие — на регламентировании разрешенного межмашинного обмена [4].

Процесс управления защитой информации при функционировании СУ ТКС и ЦОД, включает следующие этапы: этап контроля за формированием канала доступа к сети общего пользования; этап сбора информации о состоянии защиты ресурсов СУ ТКС и ЦОД; этап принятия решения по реализации конкретной задачи защиты информации (ЗИ) и доведение управляющего воздействия.

При этом МЭ в составе СЗИ для СУ ТКС и ЦОД предназначены для решения трех основных задач: защита ресурсов СУ от атак со стороны Интернет; реализация мер безопасности (для выделенного сервера/группы серверов); разделение сегментов внутренней сети управления для предотвращения попыток НСД со стороны внутреннего пользователя. Существенной особенностью МЭ в составе СЗИ для СУ ТКС и ЦОД является возможность работы с большим количеством протоколов различных уровней. Благодаря мощным встроенным языкам написания фильтров, в современных МЭ имеется возможность описать любые условия фильтрации.

Заключение. Практическая реализация современного мультипротокольного межсетевого экрана как элемента архитектуры информационной безопасностиСУ ТКС и ЦОД предопределяет возможность обеспечивать обнаружение и борьбу со всеми возможными видами атак. Благодаря этому межсетевые экраны обеспечивают высокоуровневую поддержку политики безопасности СУ ТКС и ЦОД по отношению ко всем протоколам семейства TCP/IP. Кроме того, современные межсетевые экраны характеризуются прозрачностью для легальных пользователей СУ ТКС и ЦОД, большим быстродействием и высокой эффективностью. Основной тенденцией развития средств защиты каналов и элементов СУ ТКС и ЦОД является интеграция, в частности, межсетевых экранов с криптографическими и антивирусными средствами, а также средствами анализа уровня обеспечения безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / П.Н. Дерявин, О.О. Михальский, Д.И. Правиков и др. – М.: Радио и связь, 2000. – 192 с.
2. Рынок межсетевых экранов глазами потребителей. // Межотраслевой тематический каталог «Системы безопасности», 2006. № 1 (12), С. 199-201.
3. Лукацкий А.В. Межсетевые экраны. // Технологии и средства связи, 2004, № 3. С. 72-76.
4. Авраменко В.С., Баранов В.А., Бочков М.В. Метод контроля безопасности содержимого файлов. // Телекоммуникации. 2004. № 11. С. 41-42.

УДК519.876.5

ВОПРОСЫ МОДЕЛИРОВАНИЯ СОВРЕМЕННЫХ СИСТЕМ СВЯЗИ

Беззубов Олег Владимирович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: vas@mil.ru

Аннотация. Проведен анализ задач моделирования сложных систем. Проанализированы основные методы моделирования сложных систем. Указана роль моделирования в современной науке.

Ключевые слова: *система связи; аналитическое моделирование; имитационное моделирование; математическое моделирование, метод моделирования.*

PROBLEMS OF MODELING MODERN COMMUNICATION SYSTEMS

Bezzubov Oleg
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: vas@mil.ru

Abstract. The analysis of problems of modeling of complex systems is carried out. The main methods of modeling complex systems are analyzed. The role of modeling in modern science is indicated.

Keywords: *communication system; analytical modeling; simulation; mathematical modeling, modeling method.*

В настоящее время трудно себе представить создание современной радиоэлектронной аппаратуры, аппаратуры связи и разработку систем связи без масштабного использования различных методов моделирования, идея которых состоит в том, чтобы заменить исходный объект его образом, создав математическую, имитационную модель и уже в дальнейшем решать поставленные задачи исследуя не сам объект, а его модель опираясь на различные методики и алгоритмы, реализованные на различных вычислительных средствах [1]. Данный подход позволяет учесть в себе достоинства теоретической базы и возможностей эксперимента, поскольку работа не с самим объектом (система связи), а с его моделью дает возможность относительно быстро и без затрат исследовать свойства и поведение исследуемого объекта под воздействием как внутренних факторов, так и внешних. В то же время, опираясь на современные технические средства, вычислительные эксперименты с моделями объектов позволяют, подробно и глубоко изучать объекты в форме, недоступной при реализации теоретических подходов [2,3]. Использование различных методов моделирования в современной научной деятельности является необходимым условием на фоне постоянного роста требований к эффективности устройств, применяемых в системах передачи и обработки данных, и неукоснительному требованию к сокращению сроков исследований и разработки новых инфотелекоммуникационных систем, сетей и систем связи.

Моделирование обычно выполняется с целью изучения свойств целевого объекта путем исследования его модели, а не самого целевого объекта. Можно однозначно сказать, что моделирование оправдано только в том случае, если оно проще создания самого объекта или, когда сам объект по каким-то причинам создать невозможно.

Требования, предъявляемые к модели, определяются поставленной задачей и имеющимися вычислительными средствами.

В современных условиях для повышения точности моделирования целевых объектов применяются различные методы моделирования. В зависимости от способа реализации, все модели можно разделить на несколько классов, основными из которых являются физические модели и математические модели [4].

Когда нет возможности при исследовании управляемых систем на моделирующих комплексах смоделировать аппаратуру входящую в её состав, то в состав модели включают реальную аппаратуру, также в эту замкнутую модель входят имитаторы воздействий и помех, математические модели внешней среды и процессов. Включение реальной аппаратуры или реальных систем в создаваемую модель сложных процессов позволяет уменьшить априорную неопределенность и исследовать процессы, для которых нет точного математического описания. Использование данного метода моделирования позволяет учесть в процессе моделирования параметры и характеристики существующей аппаратуры. При исследовании моделей с включением реально существующей аппаратуры используются такие понятия, как динамическое моделирование, а при исследовании сложных систем используются понятия: эволюционного, имитационного и кибернетического моделирования.

Эффективное использование моделирования в процессе создания и оценки систем связи требует серьезных вычислительных мощностей, несмотря на это, применение математических методов моделирование систем связи позволяет экономить средства на проведение исследований и испытаний разрабатываемых систем связи.

При исследовании свойств систем связи используют аналитическое и имитационное моделирование.

Основной проблемой аналитической модели систем связи, определяющая её возможность реализации только простых систем, это описание процессов, происходящих в системах связи с помощью алгебраических, интегральных и дифференциальных уравнений, приводящих к упрощению самой модели и получения от процесса моделирования, оперяющегося лишь на связь между входными и выходными параметрами неточных результатов.

Аналитическое моделирование систем связи используется только в том случае, когда необходимо получить какие-либо зависимости для определенных параметров системы связи, определения свойств системы и начальных данных [5].

Проблемой имитационного моделирования систем связи является необходимость воссоздания процесса работы смоделированной системы с сохранением структуры и алгоритма работы во времени. В свою очередь объекты, смоделированные с использованием методов имитационного моделирования в своей структуре, могут использовать дискретные и непрерывные элементы, нелинейные характеристики и случайные воздействия. Таким образом имитационное моделирование позволяет решать более сложные задачи по сравнению с аналитическим моделированием.

Для получения точных результатов моделирования сложных систем при имитационном моделировании требуется большое количество времени, это в большей степени связано с тем, что для нахождения характеристик системы требуется многократное повторение и последующая обработка данных. В свою очередь на точность оценки вероятностных критериев качества характеризующих функционирование и эффективность работы системы связи влияет качество воспроизведения случайных событий, величин и процессов.

Для оценки эффективности функционирования систем связи используются различные методы статистического моделирования, например, метод Монте-Карло, параметрическое и непараметрическое оценивание [6].

При моделировании сложных систем, таких как система связи возникает ряд проблем решение, которых позволит избежать получение в ходе исследований модели объекта недостоверных сведений.

Одна из проблем, которая касается не только имитационных, но и аналитических методов моделирования, это проблема в принятии решения о сложности моделируемой системы и необходимостью учитывать те или иные свойства и факторы влияющие или нет на исследуемые характеристики системы.

Другой проблемой моделирования сложных систем заключается в искусственном воспроизводстве случайных воздействий внешней среды. Так как динамическая система связи является стохастической, и при её моделировании необходимо точное воспроизведение случайных величин, влияющих на её работу, в противном случае, результаты, полученные при моделировании, будут не соответствовать реальным показателям [7]. Один из путей реализации данной проблемы является использование программных методов воспроизведения случайных величин.

Оценка качества модели и полученных с ее помощью результатов является ещё одной из наиболее сложных проблем. Адекватность моделей может быть оценена с помощью сравнения измерений на реальной системе и результатов экспериментов на модели.

Результаты работы модели, полученные в процессе математического моделирования, зависит от поставленных задач, от технических средств на базе которых была реализована модель, количества времени выделенного на реализацию модели, а также от выбранной модели. Одна из самых распространенных ошибок является переход к моделированию при отсутствии достаточного количества данных о поведении системы в прошлом. Одной из основных ошибок при математическом моделировании является стремление к искажению реальных условий.

СПИСОК ЛИТЕРАТУРЫ

1. Дворецкий С.И., Муромцев Ю.Л., Погонин В.А. Моделирование систем. — М.: Изд. центр “Академия”, 2009. — 320 с.
2. Самарский А.А., Михайлов А.П. Математическое моделирование: Идеи. Методы. Примеры. — М.: Физматлит, 2001. — 320 с.
3. Рубанов В.Г., Филатов А.Г. Моделирование систем учебное пособие. — Белгород: Изд–во БГТУ, 2006. — 349 с.
4. Каталевский, Д.Ю. Основы имитационного моделирования и системного анализа в управлении: учебное пособие; 2-е изд., перераб. и доп. / Д.Ю. Каталевский. — М.: Издательский дом «Дело» РАНХиГС, 2015. — 496 с., ил.
5. Баранов В.В., Бирюков М.А., Кравченко С.А., Максимов А.С., Саенко И.Б. Имитационная модель для анализа рисков информационной безопасности при проектировании ролевых схем разграничения доступа к базам данных // Актуальные проблемы обеспечения информационной безопасности. Труды межвузовской научно-практической конференции. 2017. С. 26-31
6. Куприяшкин, А.Г. Основы моделирования систем [Текст]: учеб. пособие / А.Г. Куприяшкин; Норильский индустр. ин-т. – Норильск: НИИ, 2015. – 135 с.
7. Карпов К. Имитационное модели родите систем. Введение в моделирование с Any Logic 5. — СПб.: БХВ-Петербург, 2005. 400 с.: ил.

УДК 004.7

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Безуглый Юрий Андреевич, Вершенник Алексей Васильевич
Вершенник Елена Валерьевна, Стародубцев Юрий Иванович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: sukhorukova_lena@mail.ru

Аннотация. Реализация информационного обмена между государственными органами возложена на государственные информационные системы. Организации, работающие с этими системами, обязаны выполнять требования по защите информации, предъявляемые к этим системам. Рассматривается проблема формирования системы динамической защиты государственных информационных систем.

Ключевые слова: *государственные информационные системы; система защиты информации; мониторинг*

SECURITY OFSTATE INFORMATION SYSTEMS

Bezugly Yuri, Vershennik Alex, Vershennik Elena, Starodubtsev Yuri
Military Telecommunication Academy named after the Soviet Union Marshal Budienny S.M.
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: sukhorukova_lena@mail.ru

Abstract. Implementation of information exchange between government agencies assigned to the state information systems. Organizations working with these systems must comply with the requirements of data protection applicable to these systems. The paper deals with the problems of formation of reactive armor system state information systems.

Keywords: *government information systems, information security system, monitoring*

В целях реализации полномочий государственных органов и обеспечения обмена информацией между ними в Российской Федерации созданы государственные информационные системы (ИС).

Под государственными информационными системами понимаются федеральные и региональные информационные системы, созданные на основании соответствующих федеральных законов, законов субъектов Российской Федерации, правовых актов государственных органов [1].

Деятельность государственных ИС, в которых обрабатывается информация ограниченного доступа, регулируется приказом ФСТЭК №17 от 11.02.2013 г. Согласно данному руководящему документу основными мероприятиями по организации защиты в государственных ИС являются:

формирование требований к защите информации, содержащейся в государственных ИС;

обеспечение защиты информации в ходе эксплуатации аттестованной государственной ИС;

обеспечение защиты информации при выводе из эксплуатации аттестованной государственной ИС или после принятия решения об окончании обработки информации.

В целях обеспечения выполнения перечисленных мероприятий необходимо [2]:

1. Провести классификацию ИС и определить угрозы безопасности.
2. Сформировать требования к системе защиты информации.
3. Разработать систему защиты информации информационной системы.
4. Провести внедрение системы защиты информации информационной системы.
5. Провести аттестационные испытания.

При разработке СЗИ предписано руководствоваться следующими ГОСТ:

– ГОСТ 34.601-90 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

– ГОСТ Р 51684-2000 Защита информации. Автоматизированные системы в защищенном исполнении;

– ГОСТ Р 51624-2000 Автоматизированные информационные системы в защищенном исполнении;

– ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».

Однако современное информационно-телекоммуникационное пространство претерпело существенные изменения. Во-первых, принципиально изменились технологии создания и функционирования аппаратно-программного обеспечения оборудования. Во-вторых, резко возросло количество угроз, появились их новые виды [3, 4, 5].

Кроме того, все указанные ГОСТ, при всех их достоинствах и четко описанных алгоритмах работы, требуют доработки с учетом произошедших изменений в этой области. Кроме того, в настоящее время отсутствуют регламентирующие документы, четко описывающие состав системы защиты информации, порядок ее создания и функционирования. Существуют различные способы защиты информации [3, 5], однако они не раскрывают порядка функционирования СЗИ и требования к её подсистемам.

Таким образом, возникает необходимость создания динамической системы защиты информации, позволяющей оперативно подстраиваться под быстроизменяющиеся условия функционирования объекта защиты.

Данная система должна включать в себя следующие подсистемы: мониторинга, принятия решения, управления состоянием системы защиты.

Подсистема мониторинга предназначена для предоставления информации о возможностях нарушителя и реализуемых им стратегиях действий, фиксирования источников, времени и места реализации, типа и средств деструктивных воздействий, прогнозирования способов и методов реализации деструктивных воздействий на СЗИ.

Подсистема принятия решения предназначена для анализа полученных данных в результате мониторинга и выбора оптимальных решений на текущий момент времени.

Подсистема управления состоянием системы защиты осуществляет управление состоянием, составом, структурой и порядком функционирования системы защиты и объекта защиты в части касающейся.

При этом среднее время реакции системы защиты должно быть меньше времени реализации деструктивного воздействия нарушителем информационной безопасности.

Другими словами, цикл «обнаружение деструктивного воздействия – принятие решения – реакция системы» должны опережать цикл успешной реализации деструктивного воздействия нарушителем информационной безопасности [6].

Таким образом, одним из приоритетных направлений в области обеспечения защиты информации государственной ИС является разработка динамической системы защиты информации, позволяющей оперативно подстраиваться под быстроизменяющиеся условия функционирования объекта защиты. При этом необходимо учитывать, что в современных государственных ИС процесс защиты информации требует определенных временных затрат. Одновременный мониторинг всех ресурсов государственной ИС технически сложен, а обработка и анализ данных мониторинга будет длителен по времени, что приведет к неактуальности данных к моменту их получения. Соответственно, при увеличении времени, выделяемого на мониторинг и принятия решения, временной интервал, необходимый для реализации мер по защите информации должен сокращаться. Эти факторы, несомненно, используются нарушителями информационной безопасности и позволяют добывать информацию и реализовывать деструктивные воздействия.

Для оперативного реагирования под быстроизменяющиеся условия функционирования объекта защиты необходимо решить задачу оптимального (рационального) распределения ресурсов на подсистемы мониторинга, принятия решения, реализации мер защиты в целях формирования динамической системы защиты ИС.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный Закон №149 от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации».
2. Закалкин П.В., Сагдеев А.К., Стародубцев Ю.И., Сухорукова Е.В. Проблема формирования системы динамической защиты государственных информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании Сборник научных статей: в 3-х томах. 2016. С. 239-243.
3. Вершенник А.В., Корчемкина М.Н., Куприянов Н.А., Сухорукова Е.В. анализ условий обеспечения подлинности информации при ее передаче по каналам ССОП ЕСЭ РФ// Труды Северо-Кавказского филиала Московского технического университета связи и информатики, часть II - Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2017, 441с. С. 48-53.
4. Безуглый Ю.А., Вершенник А.В., Попова А.В., Сухорукова Е.В. Основные угрозы аутентификации // Труды Северо-Кавказского филиала Московского технического университета связи и информатики, часть II - Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2017, 441с. С. 24-28.
5. Стародубцев Ю.И., Чукариков А.Г., Корсунский А.С., Сухорукова Е.В. Принципы безопасного использования инфраструктуры связи применительно к условиям техносферной войны // Интегрированные системы управления сборник научных трудов научно-технической конференции. 2016. С. 199-206.
6. Закалкин П. В., Стародубцев Ю. И. и др. Роль мониторинга в системе обнаружения, предупреждения и ликвидации последствий компьютерных атак / Журнал "Промышленные АСУ и контроллеры" №7 2013 года. С. 67-71.

УДК 621.391.1

ЗАЩИТА САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ УКВ ДИАПАЗОНА СИЛОВЫХ СТРУКТУР

Бесков Андрей Владимирович, Вотинов Михаил Леонардович, Ковайкин Юрий Владимирович, Кривошей Ольга Ивановна
Военная академия связи имени Маршала Советского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: Beskov08@mail.ru

Аннотация. в докладе рассматривается применение средств криптографической защиты информации, позволяющие создать в данной сфере метод формирования ключа по открытому УКВ каналу в режиме псевдослучайной перестройки рабочей частоты.

Ключевые слова: *TETRA; псевдослучайная перестройка рабочей частоты; средства криптографической защиты информации.*

PROTECTION OF SELF-ORGANIZINGNETWORKS IN THE RANGE OF POVER STRUCTURES

Beskov Andrey, Votinov Mikhail, Kovaykin Yuri, Krivoshey Yulia
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckystr., 3
e-mail: Beskov08@mail.ru

Abstract. *The* article deals with the use of means of cryptographic protection of information, pozvoljajut in this field a method of forming a key on the open VHF channel mode pseudo-random adjustment of working frequency.

Keywords: *TETRA; pseudo-random operation frequency tuning; means of cryptographic protection of information.*

Стандарт TETRA создавался Европейским институтом телекоммуникационных стандартов (European Telecommunications StandardsInstitute, ETSI) как единый общеевропейский стандарт

цифровой транкинговой радиосвязи. До апреля 1997 г. аббревиатура TETRA означала Транс европейское транкинговое радио (Trans-EupopeanTrunkedRAdio). Впоследствии, когда интерес к стандарту TETRA вышел за пределы Европы, смысл аббревиатуры TETRA изменился и стал расшифровываться как Наземное Транкинговое Радио (TErresstrial Trunked RAdio).

Стандарт TETRA является основным (если не сказать единственно доступным) стандартом для систем профессиональной транкинговой радиотелефонной связи. Это прежде всего современный цифровой стандарт, разработанный на основе технологии GSM и ориентированный на создание систем связи эффективно и экономично решающих задачу гибкой коммуникации между различными группами пользователей с обеспечением многоуровневой приоритезации вызовов и защищенности информации.

Основными пользователями систем стандарта TETRA являются силовые ведомства, аэропорты, производственный сектор. Радиоинтерфейс стандарта TETRA предполагает работу в стандартной сетке частот с шагом 25 кГц. Необходимый минимальный дуплексный разнос радиоканалов — 10 Мгц. Для систем стандарта TETRA могут использоваться диапазоны частот от 150 до 900 МГц,

Важным фактором привлекательности стандарта TETRA для правоохранительных органов является тщательно разработанная система обеспечения безопасности связи. Стандарт TETRA обеспечивает два уровня безопасности передаваемой информации: стандартный уровень, использующий шифрование радиоинтерфейса (обеспечивается уровень защиты информации, аналогичный системе сотовой связи GSM); высокий уровень, использующий сквозное шифрование (от источника до получателя), но все это не обеспечивает гарантированной стойкости. Рассмотрим режим псевдослучайной рабочей частоты в УКВ диапазоне. Режим ППРЧ между радиостанциями Р-187-П1 реализуется на основе стандарта ETSIEN 300 396 и текущего протокола. Протокол канального и физического уровней режима работы ППРЧ радиостанции Р-187-П1предназначен для организации помехозащищенной радиосвязи между радиостанциями Р-187-П1 и обеспечивает:

– передачу голосового трафика и данных;
– адресный и групповой (циркулярный) вызовы.

Акцент современной технической политики в сфере телекоммуникаций сделан на создании нового поколения высоконадежных систем связи. В области радиосвязи данное направление особенно ярко выразилось в реализации широкомасштабных программ создания помехозащищенных систем и средств радиосвязи, в том числе использующих режим псевдослучайной перестройки рабочих частот (ППРЧ). По существу, реализуемый в системах радиосвязи режим ППРЧ представляет собой способ расширения спектра сигнала в пределах заданной полосы частот путем скачкообразного изменения номинала несущей частоты одновременно на всех радиостанциях системы радиосвязи по априорно известному абонентам псевдослучайному закону с не исчерпываемым за время его использования периодом. При этом достигаемый эффект надежности связи определяется большим объемом используемых частот, из которого осуществляется случайный для стороннего наблюдателя выбор очередной рабочей частоты, и малым временем существования сигнала на этой частоте. Это значительно усложняет контроль (обнаружение и измерение параметров) сигналов систем связи с ППРЧ и возможность постановки преднамеренных помех. А повышение разведзащищенности и помехоустойчивости, в свою очередь, повышает надежность связи.

Условия функционирования радиолиний в системе связи характеризуется, с одной стороны, многообразием боевого применения средств и комплексов радиосвязи, многонаправленностью, широким диапазоном, неравномерностью и изменением дальностей обеспечиваемых связей, изменчивостью уровней сигналов, воздействием на линии и узлы связи средств радиоэлектронной борьбы и высокоточного оружия противника, а с другой – ограниченностью частотных, энергетических и канально-аппаратурных ресурсов, которыми располагают радиолинии и средства радиосвязи.

В то же время, к системе связи предъявляются все более высокие требования по своевременности, надежности и достоверности передачи сообщений, доставки шифрключей и их ввод в средства криптографической защиты информации. В этих условиях одним из путей повышения эффективности функционирования системы связи соединения является рациональное использование ресурсов радиолиний и средств радиосвязи и распределение шифрключа по каналу связи с помощью режима псевдослучайной перестройки рабочей частоты.

Из выше сказанного можно отметить, что для организации защищенной радиосвязи целесообразно использование встроенных в радиостанции средства криптографической защиты информации (СКЗИ). Беспроводные технологии являются эффективным и удобным инструментом передачи информации в локальных сетях. Однако открытость среды передачи требует применения специальных мер защиты информации, в том числе шифрования и аутентификации, для осуществления которых, как известно, необходимы шифрключи. Распределение ключей и управление ими представляет самостоятельную и достаточно сложную задачу, которая может быть решена в классах симметричных или асимметричных криптосистем.

Применение асимметричных ключей требует проведения вычислений с числами большой размерности, что не всегда реализуемо, если оконечные терминалы сети должны быть простыми устройствами.

Существует несколько подходов к решению задач распределения ключей для симметричных криптосистем в телекоммуникационных и компьютерных системах:

– распределение ключей с помощью курьерской службы;
– распределение ключей с использованием квантового канала;
– распределение ключей на основе использования каналов связи с шумом;

Перспективным направлением в данной сфере является метод формирования ключей по открытому УКВ радиоканалу в режиме псевдослучайной перестройки рабочей частоты.

СПИСОК ЛИТЕРАТУРЫ

1. Галкин С.Л., Коржик В.И., Юркина А.Ю., Кокосийска М.Б., Минков Б.И., КушнирД.В**.** Практическая реализация передачи ключей по волоконно-оптическому каналу связи // 47-я НТК проф.-препод. состава Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича: Тез. докл. -СПб, С.2 – 6. 1994.
2. Мельников А.А., Прохоров В.К., Бондарь О.И., Радиолинии с программной перестройкой рабочих частот. ВАС, 1989, 94с.
3. Стародубцев Ю.И., Бречко А.А., Львова Н.В., Необходимость оценки защищенности системы связи от средств информационной борьбы в современных условиях. Радиолокация, навигация, связь Сборник трудов XXIII Международной научной-технической конференции. В 3-х томах. 2017, 1201 с.

УДК 004.056.57

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕПРЕДЛОЖЕНИЯ ПО ПОВЫШЕНИЮ ЗАЩИЩЕННОСТИ ЛВСОТ КОМПЬЮТЕРНОЙ РАЗВЕДКИ

Бесков Андрей Владимирович, Кирьянов Александр Сергеевич, Ковайкин Юрий Владимирович, Наджафов Гаджи Амамдинович, Уйманов Андрей Викторович
Военная академия связи имени МаршалаСоветского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: Beskov08@mail.ru

Аннотация. В докладе рассматривается угрозы информационной безопасности и кибербезопасности. Применение, для обеспечения функционирования объектов силовых структур, информационных и коммуникационных технологий, оборудования и программного обеспечения, включая программы системы защиты.

Ключевые слова: *компьютерная разведка; локально вычислительные сети; единая сеть электросвязи.*

ORGANIZATIONAL-TECHNICALCOOPERATION POLISARIOCONTROLLED AT COMPUTER INTELLIGENCE

Beskov Andrey, Kiryanov Alexander, Kovaykin Yuri, Najafov Haji, Uimanov Andrey
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckystr., 3
e-mail: Beskov08@mail.ru

Abstract. The report considers information security threats and cyber security. Application, to ensure the functioning of power structures, information and communication technologies, equipment and software, including programs system protection.

Keywords: *computer intelligence; locally Vychislitelnye network; the unified telecommunication network.*

В настоящее время не только Россия, но и все мировое сообщество столкнулось с угрозами информационной безопасности и кибербезопасности.

Применение, для обеспечения функционирования объектов силовых структур, информационных и коммуникационных технологий, оборудования и программного обеспечения, включая программы системы защиты иностранного производства, сделало их крайне уязвимыми. И степень этой уязвимости неуклонно возрастает.

Вышесказанное позволяет заключить, что в условиях развития концепции «информационной войны» необходимо уделить серьезное внимание повышению защищенности локальных вычислительных сетей силовых структур.

Актуальность данного направления обусловлена наличием в предметной области определенных недостатков в теории и практике, которые характеризуются следующими основными факторами:с одной стороны, на объектах силовых структур используются средства вычислительной техники, сетевое и телекоммуникационное оборудование, а также программное обеспечение, включая программы систем защиты информации, импортируемые или произведенные по стандартам и лицензиям иностранных фирма с другой – в качестве каналов для передачи информации

используются ресурсы сети связи общего пользования (ССОП) ЕСЭ выходящей за пределы территории РФ.

Информационные системы силовых структур превращаются во все более привлекательную мишень для киберпреступников, а высокий уровень «импортозависимости» в области средств вычислительной техники и телекоммуникаций становится угрозой устойчивости их функционирования.

Возрастание возможностей противника проявляется в:

– росте количества угроз информационной безопасности;

– контролировании оборудования зарубежного производства их силовыми структурами, которое возможно будет содержать, не декларированные возможности;

– осуществлении контроля и перехвата информации передаваемой через узлы связи операторов ЕСЭ РФ;

– получении компьютерной разведки (КР) противника информации из баз данных ЭВМ, включенных в компьютерные сети, а также информации об особенностях их построения и функционирования;

– возможности КР иностранных государств, террористических организаций, отдельных злоумышленников по идентификации элементов систем военной связи и вскрытию их структуры;

– реализации компьютерными разведками (КР), киберподразделениями армий иностранных государств, преднамеренных деструктивных воздействий, распространению вредоносного кода, реализации аппаратных и программных закладок, а самое главное и опасное может позволить им не только управлять ЕСЭ РФ не в интересах России, но и использовать на территории России для достижения собственных целей.

Анализ имеющихся недостатков и вскрытых факторов, влияющих на защищенность локальных вычислительных сетей (ЛВС) в условиях компьютерной разведки противника как внешнего, так и внутреннего, что и определяет направлениеисследования, заключающееся в разработке организационно-технических предложений, применение которых обеспечит повышение защищенности ЛВС силовых структур в условиях компьютерной разведки противника, и наметить возможный путь ее достижения выполнением частных исследований:

1. Анализ условий функционирования ЛВС силовых структур как объекта защиты.

2. Методика исследования системы защиты ЛВС силовых структур.

3. Разработка организационно-технических предложений по повышению защищенности ЛВС силовых структур от компьютерной разведки.

Проведенный анализ функционирования ЛВС в условиях ведения КР показывает, что систему связи будет представлять ЛВС, которой теоретически присущи все угрозы ИБ как внешние, так и внутренние. Реализуются эти угрозы посредством извлечения и анализа информации (сообщений электронной почты, данных, передаваемых между разными уровнями органов управления) в процессе ее передачи;удаленным или локальным несанкционированным доступом к информации в процессе ее обработки на серверах баз данных, рабочих станциях пользователей, ее копированием и последующей передачей на пункты сбора и обработки данных разведывательных служб.

Анализ средств и способов ведения КР для которой потенциально доступными являются открытые и закрытые автоматизированные информационные и информационно-телекоммуникационные системы, показывает, что применяемые в ЛВС силовых структур средства и способы защиты ограничены и не способны в полной мере обеспечить секретность, доступность и целостность информации в процессе ее обработки, хранения и передачи.

Указанное противоречие определяет актуальность направления исследования, заключающейся в разработке организационно-технических предложений по повышению защищенности ЛВС силовых структур от КР.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальность осуществления сетевого контроля защищенности информационных сетей Лепешкин О.М., Карпов А.В., Шостак Р.К.В сборнике: Радиолокация, навигация, связь Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1198.
2. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации. 2013, с. 52
3. Лепешкин О.М., Корсунский А.С. Оптимизация структуры комплекса информационно-технических средств в автоматизированных системах управления // Автоматизация процессов управления, — 2011, — №4. с.76-81.

УДК 004.056

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСКРЕЦИОННОЙ МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ СРЕДСТВАМИ РОЛЕВОЙ МОДЕЛИ

Бирюков Михаил Александрович, Волкова Евгения Валерьевна, Саенко Игорь Борисович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: urgent.ma@gmail.com, ewgesha15@gmail.com, ibsaen@mail.ru

Аннотация. В материале рассмотрены ключевые особенности дискреционной модели управления доступом, обозначены достоинства и недостатки указанной модели. С целью устранения недостатков дискреционной модели управления доступом предложено реализовать дискреционную модель управления доступом средствами ролевой модели управления доступом. Описаны конкретные особенности построения такой ролевой модели управления доступом. Приведены выводы о достоинствах полученной реализации.

Ключевые слова: *ролевое управление доступом; защита информации; доступ; ресурсы.*

THEFEATURESOFDISCRETIONARY ACCESS CONTROLMODEL IMPLEMENTATION BY ROLE BASED ACCESS CONTROL MODEL FACILITIES

Biryukov Mikhail, Volkova Evgeniya, Saenko Igor
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: urgent.ma@gmail.com, ewgesha15@gmail.com, ibsaen@mail.ru

Abstract. The paper considers key features of the discretionary access control model and depicts its advantages and weaknesses. To eliminate weaknesses of the discretionary access control model, the paper offers to implement discretionary control model by role-based access control facilities. The specific facilities of role-based access control design are described. The advantages of such implementation are concluded.

Keywords: *role-based access control; information security; access; resources.*

Дискреционная модель управления доступом (DAC - discretionary access control, далее – дискреционная модель) – одна из наиболее простых моделей доступа в большом мире моделей безопасности. До недавнего времени эта модель имела наибольшее распространение по всему миру [1].

Основные понятия дискреционной модели – субъекты (пользователи, процессы и др.), объекты (файлы, документы) и разрешения (операции, направленные на обработку или взаимодействие с данными). Для каждой пары субъект-объект явно перечисляются доступные привилегии, определяющие санкционированные действия данного субъекта по отношению к данному объекту.

Тем не менее дискреционная модель не лишена недостатков. Важно отметить, что у каждого объекта существует владелец, который обладает полным набором прав и может делиться ими с другими субъектами. В такой «бесконтрольности» раздачи прав заключается серьезный недостаток с точки зрения безопасности. По ошибке или по злому умыслу владелец конфиденциальных данных может их легко рассекретить. Кроме этого, с увеличением количества пользователей дискреционной модели серьезно усложняется ее администрирование.

В связи с указанными недостатками появилась необходимость усовершенствования моделей доступа. В настоящее время широкое распространение получила ролевая модель управления доступом (RBAC – Role Based Access Control, далее – ролевая модель). Ролевая модель управления доступом имеет следующие преимущества [2]:

- легкая управлять и контроль ресурсов и пользователей;
- иерархичность построения и масштабируемость;
- поддержание принципа минимально необходимых привилегий;
- упрощена процедура делегирования полномочий и др.

Данная модель является естественным отражением больших структур с различной иерархией должностных лиц и их служебных обязанностей.

Чаще всего дискреционная модель реализуется в виде списков контроля доступа или матриц контроля доступа.

Для каждого файла в системе можно хранить список пар (субъект- привилегия) [3].

В терминах ролевой модели доступа также можно выразить и модель дискреционного управления доступом, и ее различные модификации. Из-за того, что дискреционная модель обладает высокой свойством высокой детализацией структуры, то размеры структуры ролевой модели существенно возрастают.

Для моделирования потребуется использовать как ролевую модель, так и административно-ролевую модель управления доступом (ARBAC - Administrative Role Based Access Control).

Рассмотрим различные виды дискреционной модели доступа:

- строгая дискреционная модель (владелец объекта не меняется. Только он «дарит» привилегии);
- нестрогая дискреционная модель (владелец может передавать другим пользователям право «дарить» привилегии);
- дискреционная модель с изменяющимся владельцем;
- дискреционная модель, в которой привилегии могут быть отозваны только тем пользователем, кто их дал, или не обязательно;

Общая концепция моделирования дискреционной модели в общем случае выражается тем, что при создании объекта О необходимо выполнить следующие действия: создать три административные роли: OWN_O, PARENT_O, PARENTwithGRANT_O и одну роль READ_O – роль-читатель [4].

Роль OWN_O – это роль которая имеет право добавлять и удалять пользователей роли PARENTwithGRANT_O. Роль PARENTwithGRANT_O имеет право добавлять/удалять пользователей роли PARENT_O.

Также необходимо создать еще несколько полномочий:

– canREAD_O. Позволяет пользователю роли READ_O читать объект;
– destroyObject_O. Право OWN_O на удаление объекта;
– add/deleteReadUser_O. Права PARENT_O на добавление удаление читателей;
– add/remParent_O. Права PARENTwithGRANT_O на добавление/удаление;
– add/remPARENTwithGRANT_O. Права OWN_O на добавление/удаление PARENT_O. PARENTwithGRANT_O.

Для удаления объекта необходимо удалить роли OWN_O, PARENT_O, PARENTwithGRANT_O, READ_O вместе с полномочиями [1].

Различные варианты дискреционной модели доступа моделируются путем введения дополнительных ролей, либо с помощью добавления ряда ограничений ролевой модели, поэтому класс моделей ролевой модели гораздо шире чем класс моделей дискреционной модели доступа.

Реализация дискреционной модели управления доступом средствами ролевой модели управления доступом позволяет с каждым объектом сопоставлять набор разрешенных операций доступа каждой роли, а не каждому пользователю. Кроме этого, реализуется возможность наследования разрешений от нижележащих ролей. Также осуществлено разделение обязанностей и минимизация используемых ресурсов.

Что касается проблемы определения безопасного состояния, то в ролевой модели они формулируются и решаются намного сложнее, нежели в дискреционной модели.

Неоспоримые плюсы ролевой модели: возможность контроля доступа с точностью до объекта; в больших организациях авторизация роли сразу для нескольких пользователей облегчает задачу управления политикой безопасности.

Отметим также, что в терминах ролевой модели очень легко реализуются принцип «минимальной привилегии» (привилегии, которая доступна всем), принцип разделения обязанностей (например, запрет активации определенных ролей одним пользователем), централизованное администрирование модели.

Проблемы в очень больших системах, увы, по-прежнему присутствуют: наличие ролевых иерархий и наследования существенно усложняют процесс управления политиками. Также существуют проблемы с контролем безопасного состояния системы

Среди современных систем, реализующих в том или ином виде ролевой подход, можно упомянуть: SELinux, MS Exchange Server 2013, MS Active Directory, Oracle Enterprise Repository и др.

В большинстве случаев концепция ролевой модели применяется для выдачи пользователям привилегий по управлению своими ресурсами в системе [5].

СПИСОК ЛИТЕРАТУРЫ

1. R.Sandhu, S.Osborn, Q. Munawer. Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies // ACM Transactions on information on information and System Security (TISSEC). Volume 3. Issue 2. May 2000. P. 85-106.
2. ЧудновА.М., КирикД.И., КурашевЗ.В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений // Радиотехнические и телекоммуникационные системы. - 2017. -№2. с.41-49.
3. Башкирцев А.С., Михайличенко Н.В., Ренсков А.А., Паращук И.Б. Совершенствование объема и номенклатуры множества контролируемых параметров, принадлежащих пространству управления информационными системами и сетями // Успехи современной науки 2017, №1, Т.4, С.46-52.
4. Неижмак А.В., Орешина М.А. Методы защиты облачных хранилищ // Образование и информационная культура: теория и практика. Материалы Межрегионального форума. Под редакцией В.Г. Шубовича. 2016. С. 88-92.
5. Овсянников С.Н., Хмелевской В.П. Организация информационного процесса в системе автоматизации управления связью // Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 389-391.

УДК 004.056

СПОСОБ РЕАЛИЗАЦИИ МАНДАТНОЙ МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ РОЛЕВОЙ МОДЕЛИ

Бирюков Михаил Александрович, Зибров Олег Павлович, Саенко Игорь Борисович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: urgent.ma@gmail.com, ibsaen@mail.ru

Аннотация. В докладе рассмотрены ключевые особенности мандатной модели управления доступом, обозначены достоинства и недостатки указанной модели. С целью устранения недостатков мандатной модели управления доступом предложено реализовать эту модель средствами ролевой модели управления доступом. Описаны конкретные особенности построения такой ролевой модели управления доступом. Приведены выводы о достоинствах полученной реализации.

Ключевые слова: *мандатное управление доступом; защита информации; доступ.*

THE METHOD OF MANDATORY ACCESS CONTROL IMPLEMENTATION BY ROLE BASED ACCESS CONTROL FACILITIES

Biryukov Mikhail, Zibrov Oleg, Saenko Igor
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: urgent.ma@gmail.com, zibrovop@mail.ru, ibsaen@mail.ru

Abstract. The paper considers key features of mandatory access control model and depicts its advantages and weaknesses. To eliminate weaknesses of mandatory access control model, the paper offers to implement mandatory access control by role-based access control model facilities. The specific facilities of role based access control design. The advantages of such implementation are concluded

Keywords: *mandatory access control; information security; access.*

В 80-х годах прошлого столетия была разработана мандатная модель управления доступом (MAC - Mandatory Access Control, далее – мандатная модель). Основная идея мандатной модели заключается в том, что конкретный пользователь (владелец) не может изменять права доступа к файлам. Система должна проверять, может ли определенный субъект работать с требуемым объектом. Цель мандатной модели – сохранение целостности и конфиденциальности информации и предотвращение возможности изменения прав доступа самими пользователями. Зачастую мандатная модель дополняет другую модель, например, дискреционную [1].

В основе мандатной модели лежит концепция MLS (multilevel secure), в которой каждый объект в системе имеет классификацию (метку безопасности), каждый субъект имеет «уровень видимости» (допуск, метка безопасности), задача системы контроля – сравнивать метки и тем самым определять возможности доступа.

Особенностями мандатной модели является то, что при большом количестве пользователей данная модель сложна в администрировании, а также в мандатной модели отдельно взятые категории одного уровня равнозначны, что приводит в большинстве случаев к избыточности прав доступа для конкретных субъектов в пределах соответствующего уровня.

В настоящее время широкое распространение получила ролевая модель управления доступом (RBAC, Role Based Access Control, далее – ролевая модель).

В терминах ролевой модели можно выразить мандатную модель управления доступом (не только классическую, но и в различных модификациях) [2,3]. Как известно, мандатная модель реализуется на решетках классов доступа с частичным отношением порядка. Модифицируем уже известное правило *Property (право собственности), подразделив его на два правила [4,5]:

1) правило 1. (нестрогое, Liberal -*Property). Субъект может записать в объект, если метка субъекта больше метки объекта.

2) правило 2. (строгое, Strict -*Property). Субъект может писать в объект только если метка субъекта равна метке субъекта.

Частным случаем мандатной модели является модель Белла-ЛаПадула. Смоделируем решетку Белла-ЛаПадула. Основная идея состоит в том, чтобы создать ролевую иерархию, соответствующую структуре решетки мандатной модели. Нужно учесть, что чем выше роль ролевой иерархии, тем больше у нее привилегий. Таким образом придется использовать две различных ролевых иерархии, чтобы удовлетворить и правилу чтения, и правилу записи в мандатной модели. Рассмотрим решетку с четырьмя метками: High, Medium 1 и Medium 2, Low. Тогда в случае моделирования мандатной модели с нестрогим правилом записи получим следующую ролевую модель [1]:

– роли для чтения и записи R = {HR, M1R, M2R, LR, HW, M1W, M2W, LW};

– ограничение на присваивание ролей: каждому пользователю присваивается ровно две роли: xR и xW (на чтение и на запись);

– ограничение на сессии: каждая сессия активирует ровно две роли: yR и yW (на чтение и на запись);

– метка чтения присваивается роли тогда и только тогда, когда метка записи присваивается роли записи;

– метка чтения присваивается ровно одной роли/

При моделировании мандатной модели со строгим правилом записи получим ту же ролевую модель, но ролевая иерархия для записи станет дискретной.

С помощью небольших поправок реализуются возможные модификации мандатной модели:

– мандатная модель с доверенным интервалом записи, в которой появляются субъекты: для чтения, для записи, причем субъектов для записи меньше чем субъектов для чтения;

– мандатная модель с независимым интервалом записи, в которой на метки чтения и записи не закладывается ограничение доминирования.

Таким образом, получена возможность проектирования мандатной модели с помощью ролевой, что позволяет упростить администрирование и избавит от избыточности прав доступа.

СПИСОК ЛИТЕРАТУРЫ

1. R.Sandhu, S.Osborn, Q. Munawer. Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies / ACM Transactions on information on information and System Security (TISSEC). Volume 3. Issue 2. May 2000. P. 85-106.
2. НеижмакА.В., ОрешинаМ.А. Методызащиты облачных хранилищ / Образование и информационная культура: теория и практика. Материалы Межрегионального форума. Под редакцией В.Г. Шубовича. 2016. С. 88-92.
3. Брунилин А.А., Бирюков М.А., Саенко И.Б. Модель и метод использования онтологий для управления разграничением доступа в едином информационном пространстве / Математические методы в технике и технологиях – ММТТ. 2016. № 6 (88). С. 122-124.
4. Калюка В.И., Овсянников С.Н., Сапунова Л.П. Оптимизация локального ресурса пропускной способности сети широкополосного радиодоступа / Наукоемкие технологии в космических исследованиях Земли. 2016. Т.8. №3, С.35-40.
5. Котенко И.В., Саенко И.Б. SIEM-системы для управления информацией и событиями безопасности // Защита информации. Инсайд. 2012. № 5 (47). С. 54-65.

УДК 681.5.015

ОРГАНИЗАЦИЯ ЗАЩИЩЁННЫХ ПРОЦЕССОВ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ

Борец Дмитрий Владимирович, Ковалев Игорь Станиславович,
Малышев Виктор Сергеевич, Пантюхин Олег Игоревич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: p_oleg99@mail.ru

Аннотация. В докладе рассматриваются моделизащищённыхинфотелекоммуникационных систем, информационные процессы и способы организации защищенных информационных процессов.

Ключевые слова: *информационный процесс; информационно-телекоммуникационная система; компьютерная сеть; защищённое распределённое преобразование информации.*

ORGANIZATION OF PROTECTING PROCESSES IN THE INFORMATION- TELECOMMUNICATION SYSTEM

Borets Dmitry,Kovalev Igor, Malyshev Viktor, Pantyukhin Oleg
Millitary Academy of Communications named S.M. Budyonnogo
Russia, St. Peterburg, Tikhoretsky pr., 3
e-mail: p_oleg99@mail.ru

Abstract. In the report models of the protected infotelekommunikatsionny systems, information processes and ways of the organization of the protected information processes are considered.

Keywords: *information process; information-telecommunication system; computer network; protected distributed information transformation.*

Толчком к появлению и развитию идеи создания инфотелекоммуникационных систем (ИТС) явилось развитие тенденций к взаимной интеграции систем автоматизации и связи (коммуникации) и интеллектуализации предоставляемых ими услуг.

По существу, ИТС - это разветвленная информационно-вычислительная сеть коллективного пользования, относящаяся к классу территориальных, коммуникационная подсистема которой позволяет наряду с передачей данных осуществлять телефонную, телеграфную, факсимильную и видеосвязь. Вопросы защиты информации в подобных сетях предполагают применение модели защищенной системы и построение на её основе защищённых информационных процессов. Модель защищенной системы должна включать в себя: модель субъектов информационной деятельности; модель объектов защиты; правила разграничения доступа.

Информационный процесс (ИП) представляет собой целенаправленную совокупность операций по преобразованию информации в пространстве и времени, реализуемых в определенной среде, начиная с момента поступления информации в систему и заканчивая ее выдачей пользователю [1].

Главным объектом преобразования в ИТС является информация. Элементарным действием в её информационном процессе является операция преобразования информации.

Управление является обязательным атрибутом обеспечения эффективного функционирования любой сложной системы. Выражение «управление ИП» не следует понимать буквально, поскольку управление осуществляется системами и лишь через них — процессами.

Проблема совершенствования ИП в распределённых системах, по существу, распадается на две взаимоувязанные подпроблемы: совершенствования системы, реализующей ИП, и разработки механизмов обеспечения её эффективного функционирования.

ИТС, функционирующая в соответствии с технологией защищённого распределённого преобразования информации (РПИ), относится к классу территориальных информационных систем коллективного пользования, входит в состав единой ИТС и является средством решения проблемы совершенствования ИП в распределённых системах.

Основными компонентами ИТС являются: коммуникационная сеть (КС), единая компьютерная сеть (ЕКС), сеть абонентских терминалов, система управления (СУ) ИТС и мобильная компонента. Взаимодействие удаленных пользователей и всех составляющих ИТС компонентов основывается на ЭМВОС.

Существенными свойствами ИП в ИТС являются: адекватность, оптимальность, оперативность, скрытность, и эффективность.

Процессный базис СУ составляют процессы: формирования (подготовки), передачи, семантической обработки, хранения и предъявления информации пользователям. Все многообразие реальных ИП строится на их всевозможных сочетаниях и различиях в последовательности. Один процесс на другой непосредственно воздействовать не может. Воздействие осуществляется лишь через реализующие системы и только на системы, являющиеся объектами воздействия [2].

Управление ИП заключается в формировании управляющих воздействий, с помощью которых достигается соответствие между текущими значениями показателей существенных свойств ИП в ИТС и требуемыми в смысле обеспечения целенаправленного движения системы в пространстве ситуаций, и осуществляется на двух уровнях: технологическом и организационном.

Опыт применения ИТС в различных сферах деятельности показал, что традиционная технология преобразования информации является не только в каком-либо смысле «неудобной» или неприспособленной для сетевого использования, но и тормозом для совершенствования организации информационных процессов в распределенных системах, а в ряде случаев она вообще не может быть применима.

Решение проблемы эффективной реализации потенциальных возможностей ИТС находятся на пути создания системы защищённого распределённого преобразования информации, которая представляет собой частное логическое образование на «фоне» ИТС, т. е. по существу, это - модель системы, реализующей прикладные процессы одной функциональной группы пользователей. Она включает в себя часть ресурсов ИТС, используемых как коллективно (КС, ЕКС, базы данных (БД) общего назначения, общее программное обеспечение (ПО) и т. п.), так и индивидуально каждой системой (абонентская система, общесистемное ПО и т. п.), а также часть ресурсов суперсистемы (локальные и распределённые БД специального назначения, специальное ПО и т. п.), являющейся коллективным пользователем ИТС, и ее должностных лиц, инициирующих и завершающих ИП соответствующей функциональной группы.

Процесс программирования (реконфигурации) виртуальной сети может осуществляться на двух уровнях: локально, на уровне РПИ, и глобально, на уровне ИТС. Необходимость двухуровневого программирования обусловлена двумя обстоятельствами. Во-первых, необходимостью обеспечения конфиденциальности и защищённости обработки информации в рамках ИТС, во-вторых, целесообразностью рационального сочетания преимуществ и компенсации недостатков, присущих принципам централизованного и децентрализованного управления.

Базовые ИП основаны на использовании стандартных моделей и инструментальных средств и могут быть использованы в качестве составной части информационной технологии. В состав базовых ИП входят операции (этапы): извлечение (сбор, ввод) информации; транспортирование информации; обработка информации; хранение информации; представление (вывод, выдача) и использование информации. Таким образом, организацию и моделирование ИП необходимо рассматривать на нескольких уровнях: концептуальном, информационном и технологическом при реализации в конкретных условиях на определенных технических и программных средствах

СПИСОК ЛИТЕРАТУРЫ

1. Анфилатов В.С., Авраменко В.С., Пантюхин О.И. Теоретические основы автоматизации управления войсками и связью. Часть 2. Основы построения и функционирования систем автоматизации управления войсками и связью: Учеб. пособие. – СПб.: ВАС, 2015г. – 304с.
2. Малышев В.С., Пантюхин О.И., Пащенко В.В., Терехин Д.В. Информационные процессы в автоматизированной системе специального назначения. Региональная информатика(РИ-2016). СПб, 26-28.10.16г.: Материалы конференции\СПОИСУ - СПб, 2016. - 599с.

3. Брунилин А.А., Бирюков М.А., Саенко И.Б. Модель и метод использования онтологий для управления разграничением доступа в едином информационном пространстве // Математические методы в технике и технологиях – ММТТ. 2016. № 6 (88). С. 122-124.
4. Агеев С.А., Шерстюк Ю.М., Саенко И.Б., Полубелова О.В. Концептуальные основы автоматизации управления защищенными мультисервисными сетями // Проблемы информационной безопасности. Компьютерные системы. 2011. № 3 С. 30-39.

УДК 681.324

ОЦЕНКА ОПЕРАТИВНОСТИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПУНКТА УПРАВЛЕНИЯ СИЛОВОГО ВЕДОМСТВА

Борец Дмитрий Владимирович, Ковалев Игорь Станиславович, Малышев Виктор Сергеевич, Пантюхин Олег Игоревич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: dima7.borets@mail.ru

Аннотация. В современных условиях управление функционированием системы невозможно без автоматизации системы управления. Сама система управления (в том числе и система управления силового ведомства) представляет собой совокупность взаимосвязанных органов и пунктов управления, а также технической основы управления. К последней относятся системы связи и автоматизации, средствами которых оборудуются ее пункты управления. При этом локальная вычислительная сеть (ЛВС) является основой системы автоматизации. Именно от качества ее функционирования будет зависеть оперативность принятия решений органами управления. В докладе предлагается методика оценки оперативности локальной вычислительной сети пунктов управления силового ведомства, основанная на оценке информационной потребности должностных лиц пункта управления. Ядром методики является модель оценки оперативности, позволяющая определить показатель оперативности обработки сообщений и сравнить его значения с требуемыми.

Ключевые слова: *пункты управления; система автоматизации; локальная вычислительная сеть.*

EVALUATION OF THE OPERABILITY OF THE LOCAL AREA NETWORK OF THE CONTROL CENTER OF THE POWER DEPARTMENT

Borets Dmitry, Kovalev Igor, Malyshev Viktor, Pantyukhin Oleg
Millitary Academy of Communications named S.M. Budyonnogo.
Russia, St. Peterburg, Tikhoretsky pr., 3
e-mail: dima7.borets@mail.ru

Abstract. In modern conditions,the control of the functioning of the system is impossiblewithoutthe automation of the control system. The managementsystem(including the management system of the power department)is a setof interrelated bodies management posts, as well as the technical basis of management. Thelatte include communication and automation system, with the means of which its control postsare equipped.While the local area network (LAN) is the basis of the automation system. It is the quality of its functioning that will determine the efficiency of decision-making by the management bodies.This report proposes a methodology for assessing the efficiency of a local area network of points of command of a power department based on an assessment of the information needs of officials of the control center. The core of the methodology is the performance evaluationmodel, whichallows to determine the rate of processing of and compare it with therequired.

Keywords: *control points; automation system; assessment of efficiency; local area network.*

В настоящее время существенно возросла ответственность должностных лиц за принятие решения по управлению элементами силового ведомства, увеличились трудности, преодолеть которые невозможно без использования всего арсенала средств, накопленных современной наукой. Состояние управления сегодня справедливо расценивается как один из важнейших показателей эффективности любых систем этого ведомства.

Автоматизация процесса управления силового ведомства имеет цель уменьшение длительности цикла управления за счет сокращения времени на добывание, сбор и обработку информации об обстановке, уменьшения доли времени и усилий, затрачиваемых на техническую и расчетно-информационную работу, документирование принятых управленческих решений, доведение задач, команд, сигналов и распоряжений до исполнителей, контроль их исполнения. Элементы средств автоматизации развертываемые на пунктах управления силового ведомства объединяются в единую систему с использованием локальной вычислительной сети и средств обмена данными.

Системы построенные на базе ЛВС имеют ряд преимуществ:

– большая пропускная способность с высокой скоростью передачи и значительная низкая вероятность ошибок;

– оперативный обмен информацией территориально разбросанных пользователей;
– использование и хранение общей базы данных;
– относительно малые затраты на создание и эксплуатацию;
– совместное использование машинных ресурсов и доступ к периферийным устройствам.

Одним из основных показателей качества функционирования ЛВС является ее оперативность, так как именно оперативность комплексно отражает ее целевое предназначение и учитывает влияние внутренних и внешних дестабилизирующих факторов. К внутренним относятся конечная надежность средств вычислительной техники (вероятность отказа) и ошибочные действия ДЛ (вероятность ошибки), а к внешним дестабилизирующее влияние вредоносного ПО.

Анализ существующих архитектур ЛВС показывает, что по сравнению с клиент-серверной или файл-серверной архитектурой трёхуровневая архитектура обеспечивает, как правило большую масштабируемость (способность вычислительной системы справляться с увеличением нагрузки, увеличивать свою производительность без структурных изменений), за счёт горизонтальной масштабируемости сервера приложений (разбиение вычислительной системы на более мелкие структурные компоненты) и мультиплексирования соединений, большую конфигурируемость за счёт изолированности уровней друг от друга, более широкие возможности по обеспечению безопасности и отказоустойчивости.

В работе проведен анализ условий функционирования ЛВС пунктов управления силового ведомства. На основе результатов анализа информационных потребностей должностных лиц силовых ведомств, сделан выбор в сторону аналитического моделирования теории массового обслуживания. Основными этапами методики оценки оперативности ЛВС пунктов управления силового ведомства являются:

– оценка информационной потребности должностных лиц ПУ при использовании ЛВС;
– разработка модели оценки оперативности;
– собственно моделирование с учетом воздействия внутренних и внешних дестабилизирующих факторов.

Ядром методики является имитационная модель оценки оперативности, позволяющая определить показатель оперативности обработки сообщений циркулирующих в физических средах подразделениях АСУ и сравнить его значения с требуемыми.

Заключение: при определении требований к оперативности ЛВС первоочередную роль играет правильная (т.е. с учетом перспектив развития системы на стадии ее функционирования) оценка информационной потребности должностных лиц ПУ силового ведомства при использовании ЛВС. Процесс формирования требований к ЛВС пункта управления оперативного силового ведомства с учетом воздействия внутренних и внешних дестабилизирующих факторов осуществляется в рамках итерационной процедуры (способ решения математических задач путем повторного применения операции), на каждом шаге которой производится оценка времени реализации стандартного цикла управления и осуществляется определение его соответствия требованиям. Проведение расчетов по оценке оперативности ЛВС пункта управления силового ведомства, с помощью предложенного метода, показало возможность применения разработанного формального аппарата для использования в практической деятельности и определения требований к производительности ЛВС.

Выводы. Таким образом, одним из основных показателей качества функционирования локальной вычислительной сети является ее оперативность, так как именно оперативность комплексно отражает ее целевое предназначение и учитывает влияние внутренних и внешних дестабилизирующих факторов. Для определения значений показателей оперативности ЛВС силового ведомства нужна методика его оценки. С помощью предложенной методики оценки у должностных лиц появится возможность находить узкие места, а, следовательно, и пути совершенствования, существующих ЛВС, а также использовать ее при разработки перспективных, удовлетворяющих требованиям.

СПИСОК ЛИТЕРАТУРЫ

1. В. Олифер «Компьютерные сети: принципы, технологии, протоколы», Учебник для ВУЗОВ.
2. Э. Таненбаум «компьютерные сети» 4-е издание Москва - Санкт-Петербург - Нижний Новгород - Воронеж Ростов-на-Дону - Екатеринбург - Самара - Киев - Харьков - Минск 2003.
3. Альянах И.Н. «Моделирование вычислительных систем»: Учебное пособие – Л.: Машиностроение. Ленингр. Отделение, 1988 - 223с.
4. Локальные вычислительные сети: Справочник, Кн.1. Принципы построения, архитектура, коммуникационные средства»: под редакцией С.В. Назарова– М.: Финансы и статистика, 1994 - 208с.
5. Учебник / Под редакцией И.Б. Саенко. СПб.: ВАС, 2010 – 520 с.Часть 2. Новые сетевые технологии в системах управления военного назначения.

УДК 004.056.2

ТЕХНИЧЕСКИЕ СРЕДСТВА ПОРАЖЕНИЯ ИНФОРМАЦИОННЫХ КОМПЛЕКСОВ

Борисов Алексей Александрович, Владимиров Дмитрий Радиевич
Военный институт (инженерно-технический) Военной академии МТО
Россия, Санкт-Петербург, ул. Захарьевская, 22
e-mails: emcborisov@mail.ru, vladimirov-dr@yandex.ru

Аннотация. В докладе рассмотрены технические параметры современных генераторов электромагнитных импульсов.

Ключевые слова: *генератор электромагнитных импульсов; электромагнитное воздействие, терроризм.*

TECHNICAL ORDNANCE OF INFORMATION SYSTEMS

BorisovAleksey, Vladimirov Dmitrii
Military Institute (engineering) of Military Academy of MTS,
Russia, St. Petersburg, Zaharievskaya, 22.
e-mails: emcborisov@mail.ru, vladimirov-dr@yandex.ru

Abstract. The paper covers technical parameters of modern electromagnetic pulse generator.

Keywords: *the generator of electromagnetic pulses; electromagnetic terrorism.*

Качественное развитие микроэлектроники и компактных энергоемких источников питания, а также все возрастающая зависимость общества в целом от информационных технологий, породило новый вид угрозы – электромагнитный терроризм. Электромагнитный терроризм заключается в оказании деструктивного электромагнитного воздействия на микропроцессорные средства с целью их разрушения или нарушения работы.

Особенностями электромагнитного терроризма является то, что он может создаваться скрытно, анонимно и на большом удалении от объекта. После себя он не оставляет запаха, разрушений, не обладает характеристиками цвета или запаха, поэтому является идеальным средством поражения для электронного оборудования.

Массо-габаритные показатели современных генераторов таковы, что генератор со всеми вспомогательными элементами может быть замаскирован под кейс, чемодан, портфель [1]. При этом малые длительности воздействующих импульсов, которые занимают достаточно широкий спектр, перекрывающий большую часть диапазонов работы, потенциальная соизмеримость частот следования импульсов с частотами смены состояний модулированного сигнала, а также дискретная природа воздействующего импульса, обусловливает высокую восприимчивость современных микропроцессорных средств к такого рода воздействиям. При высоких энергетических характеристиках электромагнитное возможно не только на антенно-фидерную систему устройств, но также и аппаратную часть ввиду формирования наводок в цепях обработки информации [2].

Электромагнитный терроризм представляет реальную угрозу для существующего микропроцессорного оборудования, а целью электромагнитного терроризма является воздействие на информацию и микропроцессорные блоки, в которых нарушение процесса обработки информации приводит к выходу из строя оборудования или иным критическим последствиям.

СПИСОК ЛИТЕРАТУРЫ

1. Пименов П.Н. Сравнительный анализ влияния сверхкороткого электромагнитного импульса на узкополосные, широкополосные, сверхширокополосные системы радиосвязи: Технологии ЭМС, 2015.
2. Фомина И.А., Михайлов В.А., Мырова Л.О., Рязановский Т.Л. Анализ функционирования бортовых вычислительных комплексов при воздействии сверхкоротких электромагнитных полей: Электросвязь № 6, 2013.

УДК 623.618

АНАЛИЗ ПРОБЛЕМ РАЗВИТИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Борисов Александр Иванович, Логинов Вячеслав Алексеевич, Пименов Алексей Сергеевич
Военная академия связи имени Маршала Советского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: B.A.I.58@yandex.ru

Аннотация. В материале рассмотрены проблемы создания автоматизированных систем специального назначения, показана необходимость комплексного подхода к развитию данной системы, обоснована важнейшая роль в этом процессе применяемой системы стандартов.

Ключевые слова: *автоматизированная система управления; средства автоматизации; информационное взаимодействие.*

ANALYSIS OF PROBLEMS OF DEVELOPMENT OF ASU OF A SPECIAL PURPOSE

Borisov Alexander, Loginov Vyacheslav, Pimenov Aleksey
Military academy of telecommunications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretskiy pr., 3
e-mail: B.A.I.58@yandex.ru

Abstract. In paper problems of creation of automated systems of a special purpose are considered, need of an integrated approach to development of this system is shown, the major role in this process of the applied system of standards is justified.

Keywords: *automated control system, automation tools, information interaction.*

Современный период развития общества характеризуется возросшей ролью управления. Использование достижения науки и техники, усложнение социальных процессов, рост объема обрабатываемой информации ужесточают требования к управлению. В современных системах управления в несколько раз увеличился общий объем циркулирующей информации, при этом время, отводимое на выработку решений по управлению, резко сократилось. Возникает противоречие в количестве обрабатываемой информации, ее анализа и уменьшении времени на принятия решения по управлению

В настоящее время успех в противостоянии сторон зависит не только от количества задействованных сил и средств, но и от оперативности и качества управления, в частности за счет использования средств автоматизации. Система управления, в которой информационный процесс реализуется с применением средств автоматизации, с целью повышения эффективности управления называется автоматизированной системой управления. Средства автоматизации, используемые в системах управления, могут быть как в стационарном, размещающие в специальных помещениях, так и в мобильном исполнении, монтируемые на специальной транспортной базе. Мобильные комплексы могут быть использованы как автономно, так и в качестве наращивания стационарной компоненты.

В различных структурах специального назначения, на сегодняшний день, используется достаточное большое количество средств автоматизации, но говорить о создании единой автоматизированной системы, удовлетворяющей потребностям органов управления для повышения оперативности управления и принимаемых решений можно лишь с натяжкой.

Это обусловлено такими факторами как большая разнородность средств автоматизации, с дублированием функциональных возможностей, использованием программного обеспечения различных производителей и др. Все это приводит к сложности организации взаимодействия, совместимости, избыточности обрабатываемой и хранимой информации, и, в конечном итоге, усложнения и увеличения цикла управления.

В настоящие время система управления специального назначения представляет собой иерархическую структуру осуществляющую на всех уровнях сбор информации ее обработку для принятия качественных решений. Разработка автоматизированных систем различного назначения, до недавнего времени, не была определена стандартами информационно-технического взаимодействия, что привело к появлению и применяю множества уникальных протоколов информационно-технического сопряжения. Взаимодействие таких систем, при их совместном использовании при создании общего информационного пространства, приводило к снижению скорости обмена информацией, увеличение времени и стоимости разработок, привлечение значительного ресурса специалистов предприятий-разработчиков и т.д., что влекло за собой дополнительные сложности при модернизации автоматизированных систем, конфигурировании и применения.

Одним из аспектов в решении описанных проблем может явится внедрение общих требования для разработки систем автоматизированного управления специального назначения таким, позволяющих сформировать единое информационное и технологическое пространство, обеспечить эксплуатацию и своевременную модернизацию. При этом единая технологическая основа должна обеспечивать уменьшение количества разрабатываемых протоколов информационно-технического сопряжения различных автоматизированными системами, что позволит сосредоточить основные усилия на развитии специального программного обеспечения.

Базовыми элементами для разработки автоматизированной системы должны стать единая операционная система, общее специальное программное обеспечение, объектная модель хранения данных, единая система управления базой данных, информационно-лингвистическое обеспечение, географическая информационная система. Кроме того, целесообразно разработать единые стандарты обмена информацией для обеспечения информационно-технического сопряжения автоматизированных систем и комплексов различного назначения в автоматизированными системами управления различного уровня. Также необходимо обеспечить разработку базовых элементов, на которых будет строиться единая технологическая основа автоматизированной системы управления, разработать единый ряд технических средств, предназначенный для применения в автоматизированных системах управления различного назначения и уровней – как для мобильного,

так и стационарных исполнения. Выполнение таких требований построенная автоматизированных систем позволит обеспечить управление силами и средствами на всех звеньях управления.

Таким образом, рассмотренные проблемы оснащения средствами и комплексами автоматизации систем управления специального назначения, безусловно, относятся к разряду организационных и решение этих проблем позволит сконцентрировать усилия в научной и технической сфере на наиболее важных направлениях и тем самым повысить эффективность управления.

СПИСОК ЛИТЕРАТУРЫ

1. Цели и задачи создания инфокоммуникационной системы специального назеачения // Легков К.Е., 2013
2. Новые информационные и сетевые технологии в системах управления военного назначения. Часть1. Новые сетевые технологии в системах управления военного назначения. Учебник / Под редакцией С.М. Одоевского. СПб.: ВАС, 2010 – 432 с.
3. Новые информационные и сетевые технологии в системах управления военного назначения.
4. Часть 2. Новые сетевые технологии в системах управления военного назначения. Учебник / Под редакцией И.Б. Саенко. СПб.: ВАС, 2010 – 520 с.

УДК 004.056.57

ХРОНОЛОГИЧЕСКИЕ ПРИЗНАКИ ЗАЩИЩЕННОСТИ СЕТИ СВЯЗИ И ЕЁ ЭЛЕМЕНТОВ ОТ КОМПЬЮТЕРНЫХ АТАК

Бречко Александр Александрович, Львова Наталия Владиславовна,
Латушко Николай Александрович
Военная академия связи имени МаршалаСоветского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: sashabreck27@gmail.com

Аннотация. В докладе рассматриваются типовые этапы компьютерных атак и признаки защищенности от них.

Ключевые слова: *компьютерная атака; защищенность сети связи; критерии защищенности.*

THE TIME SIGNS OF NETWORK AND NETWORK PARTS SECURITY IN CYBER ATTACKS

Brechko Alexandr, Lvova Nataliya, Latushko Nikolay
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckypr., 3
e-mail: sashabreck27@gmail.com

Abstract. The report describes typical stages of cybernetic attacks and its security signs.

Keywords: *cybernetic attack; networks security; security signs.*

Сети связи, её элементы характеризуются значительным числом признаков. Ниже рассматриваются хронологические признаки. Суть их заключается в изменении и динамике изменения состояния сети и её элементов с течением времени под воздействием различных факторов.

Современные сети связи являются ресурсом, который используют множество пользователей, преследующих свои цели, которые могут быть антагонистичными. Этот факт обуславливает существование компьютерных атак [1].

Как правило, любая компьютерная атака состоит из типовых этапов. Это сбор информации, сканирование, реализация атаки (эксплуатация уязвимости) и закрепление в системе [2].

Представленные этапы, как правило, реализуются в отношении отдельного элемента сети. Атака в отношении сети в целом состоит из последовательных атак на её элементы.

Следует отметить, что этапы реализуются последовательно, выполнение следующего этапа невозможно без данных, полученных на предыдущих этапах.

Первый этап – сбор информации об объекте атаки, и он может проводится различными методами. Это самый важный этап. От объема, своевременности и достоверности сведений, собранных на этом этапе, зависит успешность проведения атаки в целом.

На этом этапе производится сбор информации об оборудовании, установленном на объекте, используемых программах и их версиях. Определяется топология сети, используемые в ней протоколы и технологии. Формируется список целевых IP адресов [3].

Следующий этап – сканирование объекта атаки. Он включает в себя сканирование портов и сканирование системы на уязвимости.

Сканирование портов, как правило, проводится автоматизированными средствами. Проводится поиск открытых портов, как TCP, так и UDP, и определяются запущенные на них службы. Типовое сканирование портов заключается в попытке установления соединения на сканируемом порте.

Причем сканирование только общеизвестных номеров портов может не принести результата, тогда для повышения вероятности успешной атаки сканируются все порты, что занимает определенное время.

Далее, когда найдены открытые порты и определены запущенные на них службы, проводится поиск уязвимостей. Существуют автоматизированные средства поиска уязвимостей, позволяющие найти в системе известные уязвимости. Однако система может не иметь известных уязвимостей, тогда проводится анализ программного кода (поиск ошибок в коде), установленных на объекте атаки программ и служб. Это сложная и нетривиальная задача, которая занимает много времени. Но решив ее, вероятность успешной атаки сильно повышается, поскольку новая уязвимость будет известна только атакующему.

После того, когда найдены уязвимости происходит реализация атаки (эксплуатация уязвимости). Уязвимость позволяет загрузить и выполнить вредоносный код на атакуемой системе. Этот этап также может быть выполнен дистанционно автоматизированными средствами. Такие средства позволяют выбрать вредоносный код, доставить на объект и выполнить его.

Написание оригинального вредоносного кода повышает вероятность успешного проведения атаки в силу того, что системам защиты, основанным на сигнатурном методе детектирования, еще не известен такой код. Это также нетривиальная задача, решение которой может занять много времени.

Общей целью компьютерных атак является получение полного контроля над объектом в привилегированном режиме. Как только это случается, происходит развитие атаки. Полный нелегитимный контроль над элементом сети, или еще хуже над всей сетью, может привести не только к нарушению конфиденциальности, доступности и целостности важной информации, но и нарушить работу объектов, управление которыми, осуществляется с помощью ресурсов этой сети. Страшно представить последствия атаки, например, на сеть управления атомной электростанцией.

Следующий типовой этап – закрепление в системе. Основной целью этого этапа является создание возможности повторно и с меньшими временными затратами получить доступ к системе в случае обнаружения атаки и блокирования действий злоумышленника. На этом этапе искусственно создаются уязвимости, например, открываются новые порты, запускаются службы, меняются конфигурации на небезопасные.

Исходя из вышеописанного следует вывод, что каждый из этапов компьютерной атаки занимает определенное время. Время реализации атаки в отношении сети, помимо всего прочего, характеризуется её топологией и связностью. Поскольку сначала атакуется граничный элемент, а потом связанные с ним, тогда время вскрытия сети, состоящей только из последовательно соединенных элементов, будет складываться из времен вскрытия каждого элемента. Но если сеть полносвязная, то время её вскрытия сложится из времени вскрытия первого элемента и максимального времени вскрытия остальных элементов.

Общеизвестно, что сложные системы, которыми являются сети связи, элементы сетей связи с течением времени изменяются. Изменение местоположения элементов сети в пространстве называется мобильностью. Это классическое определение и его недостатком является учет лишь местоположения объекта и его перемещение. Сети связи и её элементы имеют множество показателей, которые меняются во времени и это не только географические координаты. Меняется топология, связность, конфигурация оборудования, настройки, устанавливаются обновления безопасности, меняются пароли, ключи и т.д. Такое изменение состояние сети, элементов сети можно назвать мобильностью в широком смысле.

Состояние объекта, когда он похож сам на себя с заданным коэффициентом сходства называется квазистационарным.

Классические критерии защищенности, основанные на мобильности объекта, имеют следующее обоснование: пусть существует некий объект, который изменяет свое местоположение и существует некий субъект, который имеет целью оказать негативное воздействие на объект, причем субъект не знает, месторасположение объекта. Тогда, если время поиска объекта больше периода смены его местоположения, то субъект воздействия оказать не сможет.

По аналогии с вышеописанным, при компьютерной атаке объект атаки будет защищен, в случае, когда злоумышленник на атаку тратит больше времени, чем объект находится в квазистационарном состоянии. Это означает, что реализация атаки, основанная на данных, полученных на предыдущих этапах, будет неэффективна в силу изменения объекта с момента получения сведений о нём, до момента реализации атаки.

Например, в течение времени разработки вредоносного кода на систему может быть установлено обновление, устраняющее эту уязвимость, тогда проводимая атака не будет эффективной. Другой пример – атака типа brute force, когда злоумышленник пытается определить пароль методом полного перебора. Если среднее время нахождения пароля больше периода смены паролей, то объект атаки будет защищен.

Заключение. Подводя общий итог, среднее время квазистационарного состояния сети или её элементов может быть использовано в качестве признаков или критериев защищенности от компьютерных атак. В этом принципе заложено противоборство двух антагонистических систем

управления. С одной стороны, злоумышленника, пытающегося реализовать атаку в кратчайшие сроки, с другой – легитимного пользователя (администратора) проводящего защитные мероприятия [4], в данном случае увеличивая время реализации потенциальной атаки или сокращая время квазистационарного состояния элементов и сети в целом.

СПИСОКЛИТЕРАТУРЫ

1. Стародубцев Ю.И. Управление качеством информационных услуг / Ю.И. Стародубцев, А.Н. Бегаев, М.А. Давлятова; под общ. ред. Ю.И. Стародубцева. – СПб.: Изд-во Политехн.ун-та, 2017. – 454 с.
2. Лепешкин О.М., Карпов А.В., Шостак Р.К.Актуальность осуществления сетевого контроля защищенности информационных сетей. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1198.
3. Коцыняк М.А., Иванов Д.А., Лаута О.С. Модель таргетированной кибернетической атаки. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 90-98.
4. Иванов В.А., Белов А.С., Гречишников Е.В., Стародубцев Ю.И., Ерышов В.Г., Алашеев В.В., Иванов И.В. Способ контроля демаскирующих признаков системы связи. Патент № 2419153 от 30.06.2009 г.

УДК:658

ОБЗОР МЕТОДОВ ШИФРОВАНИЯ

Буханов Павел Юрьевич, Смирнов Дмитрий Михайлович, Хан Георгий Георгиевич,
Бирюков Михаил Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: pavelbuh404@mail.ru

Аннотация. Вдокладе рассмотрены наиболее известные методы шифрования и дается их сравнительный анализ.

Ключевые слова: *шифрование; стойкость шифра; методы шифрования.*

OVERVIEW OF ENCRYPTION METHODS

Bukhanov Pavel, Smirnov Dmitry, Khan Georgiy, Birukov Mikhail
The S.M. BudjonnyMilitary Academy of Signal Corps,
Russia, St. Petersburg, Tikhoretskypr., 3
e-mail: pavelbuh404@mail.ru

Abstract. The paper considers the most well-known methods of encryption and gives their comparative analysis.

Keywords: *encryption; cipher resistance; encryption methods.*

В наше время общество становится информационно-обусловленным, успех любого вида деятельности все сильней зависит от знания какой-либо ценной информации и от отсутствия ее у конкурентов. Поэтому особое внимание уделяется защите информации.

Современным методом защиты информации является ее шифрование. Шифрование - преобразование информации с помощью ключа в не воспринимаемый формат в целях скрытия отзлоумышленников и понятный для пользователя, которому она предназначена [1]. Шифрование позволяет защититься от следующих рисков информационной безопасности: кража, раскрытие информации, подделка под оригинал. Разработано множество методов шифрования [2].

При сравнительном анализе алгоритмов шифрования необходимо учитывать следующие характеристики:

- практическую стойкость шифра;
- ресурсоемкость и энергоемкость;
- скорость работы.

Алгоритмы шифрования построены таким образом, что для вскрытия требуется перебор по ключевому пространству, поэтому стойкость шифра определяется длиной ключа.

Существует два класса методов шифрования: симметричный и асимметричный. В первом случае, как получатель, так и отправитель информации используют один ключ шифрования. Во втором же у отправителя закрытый ключ шифрования, а у получателя — открытый ключ для расшифровки.

В случае симметричной схемы шифрования каждый из субъектов каким-то образом должен доставить свои ключи всем остальным участникам обмена, при этом суммарное число используемых ключей будет достаточно велико при большом количестве участников обмена. Применение асимметричного алгоритма требует лишь рассылки открытых ключей всеми участниками, суммарное число ключей равно количеству участников обмена. На практике общедоступные ключи могут помещаться в специальную базу данных. При необходимости послать партнеру зашифрованное сообщение можно сделать сначала запрос его открытого ключа. Получив его, можно запустить программу шифрования, а результат ее работы послать адресату. На использовании общедоступных

ключей базируется и так называемая электронная подпись, которая позволяет однозначно идентифицировать отправителя. Сходные средства могут применяться для предотвращения внесения каких-либо корректив в сообщение на пути от отправителя к получателю.

К симметричным методам шифрования относят следующие алгоритмы: Blowfish, DES, 3DES, CAST, AES, ГОСТ. К ассиметричным относят: RSA, El-Gamal.

Алгоритм шифрования Blowfish основан в 1993 году Брюсом Шнаером. В общем случае алгоритм состоит из двух этапов — расширение ключа и шифрация/дешифрация исходных данных. Сложная схема выработки ключа сильно усложняет атаку на алгоритм, если пытаться взломать еѐ методом перебора, однако делает его непригодным для использования в системах, где ключ часто меняется, и на каждом ключе шифруется небольшие по объему данные. Алгоритм лучше всего подходит для систем, в которых на одном и том же ключе шифруются большие массивы данных.

Алгоритм шифрования DES основан в 1975 году фирмой IBM. С 1977 по 2001 г. являлся Федеральным стандартом шифрования США. Симметричный алгоритм шифрования, в котором используется один ключ, как для получателя, так и для отправителя, то есть этот ключ используется как для расшифрования, так и для шифрования. DES имеет блоки по 64 бит и 16 цикловую структуру сети Фейстеля, для шифрования использует ключ с длиной 56 бит. Алгоритм использует комбинацию нелинейных S-блоки и линейных преобразований. Основной недостаток — размер ключа всего 56 бит, что недостаточно для современного уровня развития компьютеров.

Алгоритм шифрования Triple DES (3DES) — симметричный блочный шифр, созданный в 1978 году на основе алгоритма DES, с целью устранения главного недостатка последнего — малой длины ключа (56 бит), который может быть взломан методом полного перебора. Скорость работы 3DES в 3 раза ниже, чем у DES, но криптостойкость намного выше. 3DES является простым способом устранения недостатков DES [3].

Алгоритм шифрования CAST является в некотором смысле аналогом DES. В основе этого алгоритма лежит шесть S блоков с 8-битовым входом и 32-битовым выходом. Алгоритм сложный и зависит от реализации. Главной особенностью алгоритма CAST является то, что блоки не фиксируются. Используются ключи 128 и 256 бит.

Алгоритм шифрования AES (Rijndael) разработан в 1997 году и на данный момент является Федеральным стандартом шифрования США. В основе этого алгоритма лежит симметричный блочный шифр, который работает с блоками данных длиной 128 бит и использует ключи длиной 128, 192 и 256 бит. Алгоритм может работать и с другими длинами блоков и ключей, но они в стандарт не вошли. Для шифрования в алгоритме AES применяются следующие процедуры преобразования данных: ExpandKey — вычисление раундных ключей для всех раундов; SubBytes — подстановка байтов с помощью таблицы подстановок; ShiftRows — циклический сдвиг строк в форме на различные величины; MixColumns — смешивание данных внутри каждого столбца формы; AddRoundKey — сложение ключа раунда с формой.

Алгоритм шифрования ГОСТ основан в 1989 году в СССР и в результате стал Федеральным стандартом шифрования Российской Федерации. В основе алгоритма лежит сеть Фейстеля. Использует 128 битный ключ шифрования и является надежным. Быстродействие достаточно низкое, но позволяет увеличить скорость работы за счет возможности изменения настроек со снижением криптостойкости.

Алгоритм шифрования RSA (Rivast, Shamir и Adelman, 1977 год) предполагает, что посланное закодированное сообщение может быть прочитано только адресатом. В этом алгоритме используется два ключа — открытый и закрытый. Данный алгоритм привлекателен также в случае, когда большое число субъектов должно общаться по схеме все-со-всеми.

Алгоритм шифрования El-Gamal основан в 1985 году Эль-Гамалем. Алгоритм может быть использован для решения всех трех основных задач: для шифрования данных, для формирования цифровой подписи и для согласования общего ключа. Кроме того, возможны модификации алгоритма для схем проверки пароля, доказательства идентичности сообщения и другие варианты. Безопасность этого алгоритма, также, как и алгоритма Диффи-Хеллмана, основана на трудности вычисления дискретных логарифмов. Этот алгоритм фактически использует схему Диффи-Хеллмана, чтобы сформировать общий секретный ключ для абонентов, передающих друг другу сообщение, и затем сообщение шифруется путем умножения его на этот ключ.

Заключение. Все современные алгоритмы шифрования являются высокоэффективными при использовании ключа не менее 128 бит. Однако в условиях РФ есть смысл использовать алгоритм ГОСТ 28147-89. Он имеет ключ шифрования 256 бит и является достаточно надежным. Для повышения быстродействия алгоритма можно использовать уменьшение длины ключа или уменьшение циклов использования элементов ключа. Однако при таком повышении быстродействия нет сведений об изменении криптостойкости метода. Тем не менее, такой подход часто может быть разумным, например, при необходимости шифрования данных, теряющих свою актуальность в течение нескольких часов. В случае невозможности уменьшения криптостойкости предлагается повысить быстродействие за счет распараллеливания вычислений в мультипроцессорных системах.

СПИСОК ЛИТЕРАТУРЫ

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Триумф, 2003. — 806 с.
2. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. — М.: Аст, Астрель, 2006. — 447 с.
3. Котенко И.В., Саенко И.Б. SIEM-системы для управления информацией и событиями безопасности // Защита информации. Инсайд. 2012. № 5 (47). С. 54-65.

УДК 004.056.52

ФУНКЦИОНАЛЬНО-ДИСКРЕЦИОННАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ

Валюшкина Юлия Андреевна
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, пр., Тихорецкий, 3
e-mail: julia381995@mail.ru

Аннотация. Рассмотрены основные проблемы применительно к информационной безопасности современных телекоммуникационных сетей и рассмотрена методика выбора способов реализации механизмов обеспечения информационной безопасности на основе среды радикалов.

Ключевые слова: *телекоммуникационные сети; защита информации от несанкционированного доступа; функционально-дискреционная модель; радикал.*

FUNCTIONAL-DISCRETIONARY MODEL OF ACCESS CONTROL

Valyushkina Julia
Military Academy of Communications named after SM Budennogo
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: julia381995@mail.ru

Abstract. The main problems are considered with reference to the information security of modern telecommunication networks and a method for selecting the ways to implement information security mechanisms based on the environment of radicals is considered.

Keywords: *telecommunication networks; protection of information from unauthorized access; functional-discretionary model; radical.*

Телекоммуникационные сети предполагают передачу трафика на различных уровнях иерархии, от магистральных сетей до абонентских. В ходе выполнения задач возникает необходимость в получении ресурсов, в обмене данными, но проблема любой системы заключается в ограничении прав пользователя к получению доступа к каким-либо данным. Таким образом, возникает необходимость защиты информации от несанкционированного доступа (НСД).

Для решения данной проблемы используются различные модели управления доступом, основой которых является субъектно-объектная модель. Но тогда возникает вопрос – что в определённый момент времени является субъектом, а что является объектом? Ответить на этот вопрос не представляется возможным, так как в процессе функционирования модель постоянно изменяется, и невозможно установить какую-либо закономерность для определения выполняемых ролей.

Для упрощения данной задачи вводится понятие радикала, который заменяет понятие субъекта и объекта, а также представляет собой функцию, имеющую два состояния – активное и пассивное. При решении определенной задачи нужные радикалы активируются, в то время как пассивные остаются невидимыми, тем самым получается правило, обеспечивающее доступ к ресурсам только тех лиц, которые имеют на это право.

Ключевыми характеристиками социотехнических систем управления (СТСУ) являются:

- управляемость;
- информационная согласованность;
- функциональная безопасность (ФБ):
  а) устойчивость к сбоям;
  б) устойчивость к внешнему возмущению;
- ИБ – задача защиты информации от НСД.

Для обеспечения ИБ необходимо улучшать показатели управляемости и информационной согласованности, что достигается при составлении централизованной топологии, в то время как для обеспечения ФБ необходимо повышать устойчивость к сбоям и к внешнему возмущению. Повышение эффективности СТС возможно достигнуть с помощью составления иерархической топологии, при этом происходит объединение плюсов и минусов централизованной и децентрализованной топологий. Таким образом, рассмотрим функционально-дискреционную модель управления доступом, в которой предусматривается способ создания систем на основе иерархической топологии.

Благодаря разработке ФДМ управления доступом мы получаем модель, позволяющую повышать эффективность работы систем, осуществлять контроль за всеми попытками обращения к ресурсам, не допускать случаев НСД. В связи с постоянно увеличивающемся количеством

возникающих извне угроз, информационная безопасность телекоммуникационных сетей является одной из самых важных характеристик при разработке моделей доступа, именно поэтому она требует особого внимания.

СПИСОК ЛИТЕРАТУРЫ

1. Краснокутский А.В., Лепешкин О.М., Харечкин П.В. Анализ функциональной применимости ролевой модели разграничения доступа в системах управления. «Инфокоммуникационные технологии». 2007. Т. 5. № 3. С. 162-164.
2. Лепешкин О.М., Харечкин П.В. Анализ моделей разграничения доступа, реализованных в современных социотехнических системах.
3. Лепешкин О.М., Харечкин П.В. Функционально-ролевая модель управления доступом в социотехнических системах. Известия ЮФУ. Технические науки. 2009. № 11 (100). С. 52-57.
4. Лепешкин О.М., Харечкин П.В. Подходы к обеспечению функциональной применимости ролевой модели разграничения доступа в системе управления предприятия. Информационное противодействие угрозам терроризма. 2008. № 11. С. 57-66.
5. Лепешкин О.М., Карпов А.В., Шостак Р.К. Актуальность осуществления сетевого контроля защищенности информационных сетей. В сборнике: Радиолокация, навигация, связь Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1198.

УДК 004.056.53

ПОДХОД К ПРОТИВОДЕЙСТВИЮ КОМПЬЮТЕРНЫМ АТАКАМ НАКРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СЕГМЕНТАХ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Васюков Дмитрий Юрьевич, Смыгин Александр Михайлович Митрофанов Михаил Валерьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: cmiginsam1983@gmail.com

Аннотация. В докладе рассмотрены актуальные вопросы защиты информациоот компьютерных атаки пути решения вопросов безопасности информации на критически важных информационных сегментах сети специального назначения.

Ключевые слова: *критически важные информационные сегменты; средства противодействия компьютерным атакам.*

APPROACH TO COUNTERING COMPUTER ATTACKS ON CRITICAL INFORMATION SEGMENTS OF A SPECIAL PURPOSE NETWORK

Vasyukov Dmitry, Smygin Alexander, Mitrofanov Mikhail
Military Academy of Communications
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: cmiginsam1983@gmail.com

Abstract. In report topical questions of protection of the information from computer attacks and ways of the decision of questions of safety of the information on critical information segments of a network of special appointments.

Keywords: *critical information segments; means of counteraction to computer attacks.*

В соответствии с Доктриной информационной безопасности РФ, важнейшей составляющей технологии информационной безопасности являются средства противодействия компьютерным атакам на критически важные информационные сегменты.

Под критически важными сегментами понимаются такие подсистемы и объекты НИИ, поражение которых наносит существенный ущерб функционированию экономики, национальной безопасности и национальным интересам страны

К числу основных задач типовых критически важных информационных сегментов(КВИС) относятся:

- передача и прием исходных данных для проведения расчетов;
- сбор, хранение и доставка информации на пункте управления;
- доставка, сбор и выдача управляющей информации абонентам центров управления;
- обмен информацией между абонентами пунктов и центров управления;
- организация оперативного взаимодействия и управления между КВИС по каналам связи.

Топология, состав и функции КВИС формируются на основе унифицированных информационно-телекоммуникационных средств в соответствии с требованиями к объектам управления. Способы и протоколы информационного взаимодействия абонентов КВИС, для каждого конкретного объекта управления, реализуются в схеме организации связи с абонентами, объединяющими средства измерений, сбора, обработки и передачи информации. В каждом конкретном КВИС могут использоваться дополнительные коммутационные средства, учитывающие специфику технического и программного обеспечения [1].

В настоящее время, в условиях воздействий компьютерных атак эффективность функционирования КВИС, как главного системообразующего и управляющего компонента

автоматизированных систем, во многом определяется устойчивостью функционирования КВИС сбора, обработки и передачи информации. С заменой устаревших вычислительных средств и систем связи в КВИС появилась принципиальная возможность осуществления компьютерных атак через уязвимые места в цифровом коммуникационном оборудовании и используемом программном обеспечении в режиме удаленного доступа через прозрачные сети (как для штатного оператора, так и нарушителя) на базе типовых протоколов передачи данных.

Последствием воздействия компьютерных атак могут стать блокирование управляющей информации и внедрение ложной информации, нарушение установленных регламентов сбора, обработки и передачи информации в комплексах управления, отказы и сбои в работе КВИС, а также компрометация получаемой потребителями информации.

Актуальность разработки предложения, которое позволит нейтрализовать атаки и сохранить при этом устойчивость функционирования КВИС в ходе выполнения ТЦУ, обусловлена следующими факторами:

– интенсивным развитием технологий и средств реализации компьютерных атак;

– опасностью потери устойчивости функционирования КВИС при воздействии компьютерных атак;

– вынужденной необходимостью внедрения в КВИС программно-аппаратных комплексов иностранного производства;

– невозможностью решения, проблемы в полной мере традиционными методами и средствами защиты информации, по отношению к которым совершенствуются в настоящее время средства реализации компьютерных атак [2];

– несовершенством методов и средств противостояния компьютерным атакам.

Разработка подхода противодействия компьютерным атакам на КВИС базируется на комплексном использовании положений теории защиты информации, устойчивости и надежности функционирования автоматизированных систем, моделирования сложных систем, автоматического управления, качества и достоверности информации, обнаружения компьютерных атак.

Результаты анализа современных подходов к защите информации, обеспечению надежности и устойчивости функционирования КВИС показывают, что в них не в полной мере решены следующие вопросы:

– не рассмотрены проблемы, связанные с разработкой методов и моделей противодействия компьютерным атакам на средства сбора, обработки и передачи информации КВИС, интеллектуальных средств контроля состояния информационно-вычислительного процесса и организацией активного противодействия компьютерным атакам;

– большинство известных методов и моделей обнаружения атак не учитывают взаимосвязанное решение вопросов противодействия компьютерным атакам и устойчивости функционирования КВИС при выполнении ТЦУ;

– практически отсутствуют комплексные методы, модели и алгоритмы, в которых, на ряду с сигнатурным анализом атак и выявлением аномалий в КВИС, обнаружение атак осуществляется путем функционального анализа контролируемых параметров и идентификации состояния устойчивости функционирования КВИС;

– недостаточно проработаны методы и модели принятия решений, в том числе статистических, по обеспечению активного противодействия источникам атак.

Кроме того, используемые в настоящее время методы и модели противодействия компьютерным атакам на КВИС не разрешают ряд противоречий:

– между повышением оперативности и устойчивости системы управления, с одной стороны, и ухудшением процессов управления при воздействии компьютерных атак на КВИС, с другой;

– между уменьшением количества факторов уязвимостей КВИС, требующих устранения избыточных функций и параметров, с одной стороны, и усложнением процессов контроля информационно-вычислительного процесса в КВИС и обнаружения атак, с другой;

– между требованиями к своевременности технологического цикла управления, с одной стороны, и временем, необходимым для обнаружения и нейтрализации источника атаки, с другой.

Одним из возможных путей создания КВИС, защищенных от воздействия компьютерных атак, является интеграцияинформационных технологий КВИС с внедренными в ее структуру датчиками СПКА (средства противодействия компьютерным атакам), с соблюдением обязательного взаимодействия средств администрирования с управляющими программами СПКА. При этом эффект состояния защищенности КВИС будет достигнут тогда, когда наряду с компонентами СПКА осуществляется комплексное использование организационно-технических мер, максимальное применение средств администрирования и мониторинга сети, используются антивирусныесредства, сертифицированное программное обеспечение, компьютерное и коммутационное оборудование. Кроме того, необходимо составить перечень критических контролируемых параметров КВИС, определить их чувствительность к воздействию КА, экспериментально проверить согласованность работы компонентов КВИС,СПКА, средств защиты информации от несанкционированного доступа при выполнении реальных технологических циклов управления КА, и на основании изменений

контролируемых параметров разработать(уточнить) технические решения [3].Это позволит решить вопрос обеспечения информационной безопасности и защиты информации на критически важных сегментах сети специального назначения.

СПИСОК ЛИТЕРАТУРЫ

1. «Методы и модели противодействия компьютерным атакам» С.М. Климов Москва 2008,
2. «Системный анализ в защите информации» учеб. Пособие для студентов вузов А.А. Шумский, А.А. Шелупанов.-М.: Гелиос АРВ, 2005,
3. Обеспечение защиты информации в локальных вычислительных сетяхБударин Э.А., Васюков Д.Ю., Дементьев В.Е., Колбасова Г.С., Краснов В.А., Лепешкин О.М., Лаута О.С., Митрофанов М.В., Худайназаров Ю.К. ВАС им. Маршала Советского Союза С.М.Буденного. Санкт-Петербург, 2013.

УДК621.391(075.8)

БЕЗОПАСНОСТЬ — ПРОБЛЕМА ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА

Вертепов Михаил Васильевич, Букреев Денис Дмитриевич, Гавриленко Владимир Андреевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: b01c@mail.ru, bukreee7@mail.ru, gva007@mail.ru

Аннотация. Предпринята попытка анализа пользовательского интерфейса как бреши в безопасности операционных систем. Рассмотрены модели безопасности.

Ключевые слова: *информационная безопасность; Linux; VMS.*

SECURITYISTHEPROBLEMOFTHEUSERINTERFACE

VertepovMikhail, BukreevDenis, GavrilenkoVladimir
S.M. Budjonny Military Academy of the Signal Corps
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: b01c@mail.ru

Abstract. An attempt is made to analyze the user interface as a security hole in operating systems. Security models are considered.

Keywords: *information security; Linux; VMS.*

Говорят, естьоченьпростойспособобезопаситькомпьютерс Windows — простовыключитьего. Заэтойшуткойскрываетсясерьезнаямысль. А именно — очень просто создать безопасную систему, если вы пойдете на компромисс с функциональностью. Машина, которая ничего не делает, очень безопасна по своей природе. Проблема, стоящая перед разработчиками программного обеспечения, заключается в том, как сбалансировать удобство и безопасность [1].

Многие люди утверждают, что UNIX является более безопасной, чем Windows. Однако, когда требуют доказательств, они находят, что очень трудно указать на уязвимости в ядре NT. Действительно, на бумаге модель безопасности Windows явно превосходна — каждый объект имеет связанный список контроля доступа, и этот список проверяется ядром при каждой попытке доступа.

Модель UNIX, напротив, гораздо более примитивна [2]. Только файлы имеют какой-либо контроль доступа (хотя, по справедливости говоря, большинство вещей в системе UNIX являются, как правило, файлами), который просто имеет разрешения для пользователя, группы, и всех.

Есть только два уровня безопасности:

– Пользователи могут делать все, что им позволил делать root:
– Root может делать все.

Опыт подсказывает, что более простая модель обеспечивает большую безопасность, но это не всегда так. Например, VMS имеет одновременно подробную модель безопасности и превосходную репутацию по безопасности. Разница между VMS и Windows заключается в том, что VMS машины, как правило, запускаются людьми с большим опытом настройки и конфигурирования VMS [3]. Если большая часть вашей работы — это понимание деталей модели безопасности, то вы, вероятно, придете к хорошему обеспечению безопасности этой системы. В отличие от этого, большое количество машин с Windows — это домашние машины, запускаемые людьми с маленькими познаниями в компьютерах или же вообще без знаний, или в небольших компаниях, не имеющих IT-персонала. Если пользователи VMS настраивают свою политику безопасности осторожно, то пользователи Windows попросту отключают меры безопасности, поскольку они слишком сложны для корректной настройки.

Возможно, ту же самую критику можно перенести и на UNIX. Чтобы сравнение было справедливым, давайте взглянем на Mac OS X [3,4]. Построенная на ядре UNIX (хотя и не особенно традиционном во многих отношениях), OS X наследует модель безопасности UNIX. В OS X, система не препятствует пользователю в 90% случаев из того, что ему может потребоваться в повседневной деятельности. Для других видов деятельности, таких как установка обновлений, пользователю

предлагается ввести пароль. Другими словами, система обеспечения безопасности держится в стороне от пути пользователя большую часть времени.

В настоящее время цель большинства исследований безопасности в проектировании систем, которые трудно взломать с технической точки зрения, полностью игнорируя тот факт, что в большинстве систем пользователь является самым слабым звеном.

В настоящее время, многие системы «достаточно безопасны» с технической точки зрения, но большинство этих систем имеет пользовательские интерфейсы поверх них, что серьезно препятствуют их безопасности. Я хотел бы видеть систему, которая представляет новый подход к пользовательскому интерфейсу для безопасности, но все кажутся сосредоточенными на соревновании, чтобы видеть, кто может предоставить конечному пользователю самые запутывающие варианты выбора, и наибольшее количество причин отключить сами системы, обозначаемые как «необходимые».

СПИСОК ЛИТЕРАТУРЫ

1. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебн. пособие / Бузов Г.А., Калинин С.В., Кондратьев А.В.- М.: Горячая линия - Телеком, 2005. - 416 с.
2. Запечников С.В. Информационная безопасность открытых систем. Часть 1: Учебник для вузов / Запечников С.В., Милославская Н.Г., Толстой А.И.
3. Будников С.А., Паршин Н.В. Информационная безопасность автоматизированных систем: Учебное пособие, издание второе, дополненное -Издательство им."Е.А.Болховитинова, Воронеж, 2011.
4. Саенко И.Б., Бирюков М.А. Методика интеграции локальных схем разграничения доступа к разнородным ресурсам единого информационного пространства // Информационные технологии в управлении (ИТУ-2016) Материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В.Г. Пешехонов. 2016. С. 758-762.

УДК 004.7

СПОСОБ ЗАЩИТЫ АБОНЕНТСКИХ ЛИНИЙ

Вершенник Алексей Васильевич, Вершенник Елена Валерьевна,
Куприянов Никита Алексеевич, Стародубцев Юрий Иванович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: sukhorukova_lena@mail.ru

Аннотация. В работе рассматривается способ обнаружения несанкционированно установленных радиоэлектронных средств на абонентских линиях связи, который может быть использован для выявления технических каналов утечки конфиденциальной информации, образованных с помощью несанкционированно установленных на абонентских линиях радиоэлектронных средств

Ключевые слова: *технический канал утечки; электронное устройство; радиоэлектронное средство.*

METHOD OF PROTECTING SUBSCRIBER LINES

Vershennik Alex, Vershennik Elena,Kupriyanov Nikita, Starodubtsev Yuri
Military Telecommunication Academy named after the Soviet Union Marshal Budienny S. M.
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: sukhorukova_lena@mail.ru

Abstract. The paper discusses a method for detecting unauthorized radio electronic equipment installed on subscriber lines, which can be used to identify technical channels of leakage of confidential information, formed using unauthorized installed on subscriber lines, electronic means

Keywords: *technical channel leakage; electronic device; electronic means.*

Современный этап развития российского общества характеризуется существенным возрастанием роли и актуальности проблем обеспечения безопасности во всех сферах жизнедеятельности. Особенно показателен этот процесс для сферы информационной безопасности (ИБ), которая за последние десятилетия превратилась в мощный сегмент рыночной индустрии современных информационно-телекоммуникационных технологий.

В связи с тем, что информация является предметом собственности, неизбежно возникает проблема угрозы безопасности этой информации, заключающейся в неконтролируемом ее распространении, в хищении, несанкционированном уничтожении, искажении, блокировании доступа к информации. Следовательно, возникает проблема защиты информации (ЗИ) и ее носителей от несанкционированных воздействий, а также предотвращения других форм незаконного вмешательства в информационные ресурсы и информационные системы [1].

Одной из важнейших задач ЗИ от ее негласного добывания является контроль защищенности информации, целью которого является выявление потенциальных естественных и искусственных

(созданных с помощью средств негласного съема информации) технических каналов утечки информации [2].

Для перехвата телефонных разговоров наиболее часто используется электрический канал перехвата информации. Электрический канал перехвата информации, передаваемой по кабельным (проводным) линиям связи, предполагает контактное подключение аппаратуры перехвата к кабельным линиям связи [1].

При этом подключение к абонентским линиям автоматических телефонных станций (АТС) несанкционированно установленных радиоэлектронных средств (НУРЭС) может осуществляться как параллельно, так и последовательно.

При последовательном включении питание НУРЭС осуществляется от автоматических средств коммутации, что обеспечивает неограниченное время ее работы. Однако НУРЭС с последовательным подключением потенциально можно обнаружить за счет изменения параметров линии, в частности, падения напряжения, но при этом необходимо отличать абонентское оборудование. В ряде случаев используется последовательное подключение с компенсацией падения напряжения, но реализация этого способа требует наличия дополнительного источника питания.

НУРЭС с параллельным подключением к линии также могут питаться от абонентской линии. Чем выше входное сопротивление НУРЭС, тем незначительнее изменение параметров линии и тем труднее ее обнаружить.

Перехваченную с абонентской линии информации НУРЭС в большинстве случаев передают по радиоканалу. В качестве антенны может использоваться собственная антенна или абонентская линия. Для передачи информации наиболее часто используются VHF (метровый), UHF (дециметровый), GHz (ГГц) диапазоны длин волн и частотная широкополосная (WFM) или узкополосная (NFM) модуляция сигнала [3]. При этом необходимо отличать сигнал, передаваемый радиозакладкой от общего фона радиозагрузки в диапазоне работы закладок.

Существуют различные способы защиты информации от утечки по техническим каналам [1 – 6], однако они обладают рядом недостатков, основным из которых является низкая достоверность обнаружения и идентификации НУРЭУ. При этом НУРЭУ может быть не обнаружено в случае совпадения частоты ее радиоизлучения и расписания работы с частотой излучения и расписанием работы санкционированно установленных на объекте электронных установок. Кроме того, в случае обнаружения на объекте радиоизлучения электронной установки неизвестного типа возникает неопределенность еще и относительно назначения указанной установки, т.к. зачастую применяется ограниченная совокупность признакового пространства, и не предусматривается учет данных о спектральных составляющих радиоизлучений санкционированно установленных радиоэлектронных установок и расписании их работы.

Таким образом, возникает необходимость разработки способов обнаружения несанкционированно установленных радиоэлектронных средств на абонентских линиях связи при отсутствии предварительных данных о параметрах устройств.

Авторами предлагается способ, который может быть реализован следующим образом [6]:

К блоку питания автоматической телефонной станции (АТС) подключают генератор низкочастотного переменного синусоидального напряжения с частотой, не кратной напряжению питающей сети.

В районе расположения АТС, устанавливают широкополосный сканирующий приёмник, работающий в диапазонах частот, охватывающих потенциально возможный диапазон работы НУРЭС, возможно подключенных к абонентским линиям.

Выбирают абонентскую линию, подключенную к АТС.

К абонентской линии подключают генератор переменного синусоидального напряжения и накладывают на постоянное напряжение питания абонентской линии специализированный сигнал с уникальной частотой и амплитудой, не выходящими за пределы требований документов, регламентирующих возможный диапазон изменения питающих напряжений, т.е. не влияющих на работоспособность абонентской линии и оконечных устройств.

Включают широкополосный сканирующий радиоприемник в режиме сканирования в заданном диапазоне частот.

Принимают все электромагнитные сигналы в полосе частот, заданной для мониторинга. Прием осуществляется до того момента, пока не будет полностью осуществлен анализ всего диапазона частот. Анализируют характеристики принятых электромагнитных сигналов.

Выявляют сигнал, включающий спектральные составляющие с частотой специализированного (наложенного) сигнала. В случае, если сигнал обнаружен, локализуют абонентскую линию. Абонентская линия отключается от АТС до момента обнаружения и снятия НУРЭС. Далее переходят к анализу следующей абонентской линии.

Заключение. Таким образом, за счет искажения исходного состояния параметров излучения несанкционированно установленных на абонентской линии радиоэлектронных средств, приводящее к появлению демаскирующих признаков в структуре их электромагнитных сигналов, повышается

вероятность их определения при заранее неизвестных исходных параметрах электромагнитных сигналов.

СПИСОК ЛИТЕРАТУРЫ

1. Лобашев, А.К. Защита информации от утечек по техническим каналам. [Электронный ресурс]: – URL: http/ http://mascom-uc.ru/library/354/. Дата обращения 29.08.2017 г.
2. Стародубцев, Ю.И. Управление качеством информационных услуг / А.Н. Бегаев, М.А. Давлятова, Ю.И. Стародубцев// – СПб.: Изд-во Политехн. Ун-та, 2017. – 454 с.
3. Хорев, А.А. Техническая защита информации т.1. / А.А. Хорев // – Москва.: НПЦ «Аналитика», 2008.
4. Беликова И.С., Закалкин П.В., Стародубцев Ю.И., Сухорукова Е.В. Способ обнаружения электронных устройств несанкционированно установленных в контролируемой зоне / // Фундаментальные и прикладные проблемы техники и технологии. – 2016. – № 5 (319). – С. 150-156.
5. Стародубцев Ю.И., Сухорукова Е.В., Корсунский А.С., Масленникова Т.Н., Вершенник А.В. Задача обнаружения несанкционированно установленных радиоэлектронных устройств и способ ее решения // Автоматизация процессов управления. 2017. № 2 (48). С. 4-9.
6. Патент 2558333 Российская Федерация, МПК G01S 3/02. Способ определения местоположения несанкционированно установленных на объекте электронных устройств. /Закалкин П.В., Савченко Ю.Е., Стародубцев Ю.И., Сухорукова Е.В., Панкова Н.В.; заявитель и патентообладатель ФГБОУ ВПО «Санкт-Петербургский государственный торгово-экономический университет». – 2014112381/07; заявл. 31.03.2014; опубл. 27.07.2015. – 21 с.
7. Патент 2621455 Российская Федерация, МПК G01R 29/08. Способ обнаружения несанкционированно установленных радиоэлектронных средств на абонентских линиях связи. / Закалкин П.В., Куприянов Н.А., Стародубцев П.Ю., Стародубцев Ю.И., Сухорукова Е.В.; Зявитель и патентообладатель Стародубцев Пётр Юрьевич. – 2016119180; заявл. 17.05.2016; опубл 06.06.2017. – 13 с.

УДК 004.056

КОНЦЕПТУАЛЬНЫЕ ПОДХОДЫ К ПРОБЛЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЛЕКСОВ С БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ

Винокуров Александр Владимирович, Лозовский Владимир Валерьевич,
Кибенко Александр Викторович
Краснодарское высшее военное училище им. генерала армии С.М. Штеменко
Россия, Краснодар, ул. Красина, 4
e-mail: VAV73@rambler.ru

Аннотация. Предложены концептуальные подходы к обеспечению информационной безопасности комплексов с беспилотными летательными аппаратами. Обоснована методология исследования, основанная на совместном использовании теории адаптивных систем управления и кибернетики.

Ключевые слова: информационная безопасность; комплексы с беспилотными летательными аппаратами; концептуальные подходы; субъект и объект угроз.

CONCEPTUAL APPROACHES TO THE PROBLEM OF ENSURING INFORMATION SECURITY OF COMPLEXES WITH UNMANNED AERIAL VEHICLES

Vinokurov Aleksandr, Lozovskiy Vladimir, Kibenko Aleksandr
The Krasnodar Higher Military School named after army General S.M. Schtemenko
Russia, Krasnodar, Krasina str., 4
e-mail: VAV73@rambler.ru

Abstract. Conceptual approaches to the information security of complexes with unmanned aerial vehicles are proposed. The methodology of research based on the joint use of the theory of adaptive control systems and cybernetics.

Keywords: *information security; complexes with unmanned aerial vehicles; conceptual approaches; subject and object of threats.*

Рост популярности беспилотных летательных аппаратов (БЛА) является одной из самых заметных в мире тенденций. В тоже время, развитие и совершенствование новых информационных технологий приводит и к появлению новых угроз. Обеспечение информационной безопасности комплексов с беспилотными летательными аппаратами (КБЛА) в общей постановке проблемы может быть достигнуто лишь при взаимоувязанном решении трех составляющих проблем [1]:

– защита циркулирующей в КБЛА информации от дестабилизирующего воздействия внешних и внутренних угроз;

– защита элементов КБЛА от дестабилизирующего воздействия внешних и внутренних информационных угроз;

– защита внешней среды от информационных угроз со стороны КБЛА.

Анализ методов обработки и защиты информации КБЛА выявил отсутствие:

– принципов защиты информации в робототехнических комплексах, включая КБЛА;

– научно-методического аппарата описания информационных процессов, протекающих КБЛА;

– методология комплексной обработки и защиты информации в КБЛА;

– единого методологического базиса построения моделей информационной безопасности КБЛА и нарушителя;

– системно обоснованных показателей качества информации в КБЛА и критериев эффективности системы ее защиты.

КБЛА являются робототехническими комплексами и система защиты информации относится к системе организационно-технологического типа, т.к. общую организацию защиты и решение отдельных задач осуществляет персонал пунктов управления, а защита информации осуществляется параллельно с технологическими процессами ее обработки, но, несмотря на большое разнообразие методов защиты информации в автоматизированных системах, вопросы информационной безопасности робототехнических комплексов, включая КБЛА, рассмотрены недостаточно, что определяет актуальность разработки основных положений теории информационной безопасности КБЛА и научно-методического аппарата защиты информации, циркулирующей в них.

Основными составляющими теории информационной безопасности КБЛА являются: формирование единой терминологии и определений, классификации объектов обработки и защиты информации, методов выявления угроз информационной безопасности, принципов построения системы защиты информации, методов и средств защиты информации и оценки ее эффективности, формирование системы показателей качества.

БЛА, являясь элементом техносферы, при определенных негативных воздействиях на них могут наносить ущерб ее безопасности.

Таким образом, проблема информационной безопасности КБЛА декомпозируем по двум направлениям: рассмотрение БЛА как субъекта угроз, а с другой стороны, рассмотрение его как объекта, на который направлены деструктивных воздействий [2].

Системообразующими составляющими теории информационной безопасности КБЛА выступают основные положения теории информационной безопасности автоматизированных систем управления, теории систем, техносферной безопасности, кибернетики, теории информации, кодирования и криптографии.

Многоаспектный характер исследования КБЛА, как объекта со сложной структурой, реализующим при функционировании нелинейные, нестационарные, многосвязные зависимости, определяет целесообразность применения системного подхода, как методологии научного познания, в основе которого лежит рассмотрение объектов как систем.

Используя теорию систем и защиты информации сформулируем основные принципы организации защиты информации в КБЛА:

– конечной цели (создания системы защиты информации КБЛА для достижения максимальной эффективности функционированию КБЛА, то есть, сохранения требуемого качества информационного обеспечения, где под качеством понимается не только обеспечение его защищенности, но и ценности);

– обоснованности защиты информации (определение информационных потоков, подлежащих защите, нахождение компромисса в защите исходя из ресурсов надсистемы);

– гарантированного результата (защита информации должна обеспечивать ее требуемое качество в любых условиях обстановки, включая неопределенность влияющих факторов);

– оптимального перераспределения сил (затраты на защиту должны соответствовать уровню угроз и вероятности их появления);

– согласованности мер защиты (противодействие БЛА нарушителя должно носить целенаправленный характер и не влиять на функционирование легитимных средств).

Так как КБЛА являются динамическими системами с наличием прямых и обратных связей то целесообразно их исследование с использованием кибернетического подхода, как наиболее развитого подхода к реализации процессов принятия управленческих решений в сложных организационно-технических системах. При этом кибернетический подход применим не только для оптимизации управления БЛА, но и для управления защищенностью информации.

Рассмотрение функционирования и развития КБЛА в тесном взаимодействии с внешней средой определяет ситуационный подход [3]. Формирование условий, в которых применение тех или иных принципов приносит желаемый результат, определяется управленческой ситуацией, обозначающей совокупность всех внешних и внутренних факторов (воздействий), которые определяют условия функционирования КБЛА и их элементов, а также методов обработки информационных потоков. На основе определения стандартных управленческих ситуаций становится возможным предъявление оптимальных требований к типу организационной структуры, технологии и способов управления, методов обработки информации и т.д.

Заключение. Таким образом, состав научно-методологических основ определяется следующим образом:

– так как речь идет об организации и построении комплексной системы защиты информации, то общеметодологической основой будут выступать основные положения теории защиты информации и теории систем;

– так как речь идет об управлении защищенностью информации, то в качестве научно-методической основы будут выступать общие законы кибернетики;

– так как информация в КБЛА передается по радиоканалу, подверженному случайным помехам и целенаправленному воздействию со стороны нарушителя, то для ее защиты должны применяться основные положения теорий сигналов, информации, кодирования и криптографии;

– так как процессы обработки и защиты информации связаны с решением оптимизационных задач по распределению ресурсов, то в основе должны быть положения теории принятия решений.

СПИСОК ЛИТЕРАТУРЫ

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М. : Горячая линия – Телеком, 2004. – 280 с.
2. Винокуров А.В. Разработка и совершенствование методов защиты информационного обеспечения комплексов с беспилотными летательными аппаратами как задача противодействия информационному терроризму // Материалы Южного форума информационной безопасности Инфофорум-Крым URL: https://infoforum.ru/conference/sevastopol-17. (дата обращения 05.09.2017).
3. Поспелов, Д.А. Ситуационное управление: теория и практика. – М.: Наука. – Гл. ред. физ.-мат. лит., 1986. – 288 с.
4. Бардаев Э.А., Ловцов Д.А. Ситуационное управление защищенностью ИПО АСУ // НТИ. Серия 2. Инфор. процессы и системы. ВИНИТИ РАН, 1999. – № 11. – С. 10-21.

УДК 004.056.2

ЗАЩИТА МИКРОПРОЦЕССОРНЫХ СРЕДСТВ ОБРАБОТКИ ДАННЫХ ОТ ПРЕДНАМЕРЕННЫХ СИЛОВЫХ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЙ

Владимиров Дмитрий Радиевич, Борисов Алексей Александрович
Военный институт (инженерно-технический) Военной академии МТО
Россия, Санкт-Петербург, ул. Захарьевская, 22
e-mails: vladimirov-dr@yandex.ru, emcborisov@mail.ru

Аннотация. В докладе рассмотрена проблема обеспечения защиты микропроцессорных средств от нового вида поражающего фактора – преднамеренных силовых деструктивных воздействий.

Ключевые слова: *микропроцессорное средство; электромагнитное воздействие, терроризм*

PROTECTION OF MICROPROCESSOR MEANS OF DATA PROCESSING FROM INTENTIONAL POWER ELECTROMAGNETIC INFLUENCES

Vladimirov Dmitrii, Borisov Aleksey
Military Institute (engineering) of Military Academy of MTS
Russia, St. Petersburg, Zaharievskaya, 22
e-mails: vladimirov-dr@yandex.ru, emcborisov@mail.ru

Abstract. The paper considers the problem of providing protection microprocessor means from a new type striking factor – the power of intentional destructive impacts.

Keywords: *microprocessormeans; electromagnetic; terrorism.*

Интенсивное развитие микропроцессорных средств приводят к необходимости рассмотрения вопроса их защиты и устойчивого функционирования в условиях преднамеренного силового электромагнитного воздействия.

Особую угрозу для микропроцессорных средств представляют сверхкороткие электромагнитные импульсы (СКИ).

Ввиду длительности СКИ менее 10 нс, у данного вида воздействий активная ширина спектра поражения достигает нескольких ГГц.

Более того, применение высокоскоростных полупроводниковых ключей позволяет уменьшить длительности таких импульсов до 0,15 нс с закономерным расширением ширины спектра образующейся помехи и обеспечением высокой повторяемости характеристик генерируемых импульсов с возможностью точного задания интервалов между ними [1].

Опасность СКИ для современных микропроцессорных средств заключается в перекрытии спектром наведенной помехи рабочих сигналов в информационных цепях [2].

Анализ влияния СКИ на микропроцессорные средства позволяет заявить об их высокой уязвимости и необходимости обеспечения их защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Фомина И.А., Михайлов В.А., Мырова Л.О., Рязановский Т.Л. Анализ функционирования бортовых вычислительных комплексов при воздействии сверхкоротких электромагнитных полей: Электросвязь № 6, 2013.
2. Юдин В.Н. Принципы создания противонавигационного поля радиопомех: Журнал «Труды МАИ», 2015.

УДК519.876.5

О СПОСОБАХ МОДЕЛИРОВАНИЯ СЕТЕЙ СВЯЗИ

Волкова Евгения Валерьевна, Чукариков Александр Геннадьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: ewgesha15@gmail.com

Аннотация. Проведен анализ способов моделирования сетей связи. Проанализирован алгоритм моделирования сетей связи.

Ключевые слова: *система связи; аналитическое моделирование; имитационное моделирование; математическое моделирование, метод моделирования*

ABOUT THE COMMUNICATION NETWORK MODELLING FACILITIES

Volkova Evgenia, Chukarikov Aleksandr
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: vas@mail.ru

Abstract. The analysis of problems of modeling of complex systems is carried out. The main methods of modeling complex systems are analyzed. The role of modeling in modern science is indicated.

Keywords: *communication system; analytical modeling; simulation; mathematical modeling; modeling method.*

В настоящее время известно множество способов моделирования сетей связи (далее СС), с учетом перемещения абонентов СС, вероятности смены узлов СС, обслуживающих данных абонентов, возможности имитации перемещения элементов и абонентов СС, топологии СС и изменения емкости каналов (линий) СС и ряда других [1].

Недостатком перечисленных выше способов является то, что при моделировании сети связи не учитываются области, недоступные для связи, а также топологические неоднородности, возникающие в процессе развития сети связи, что снижает адекватность и достоверность моделирования. (Неоднородность – неравномерность свойств, разрывность, наличие разнородных элементов. Топологическая структура – взаимное расположение элементов СС на местности).

В реальных условиях должностным лицам органов военного управления часто требуется проводить моделирование с учетом характеристик реальных СС. Существует способ с повышенной достоверностью и адекватностью моделирования, а также имеет возможность моделирования типовых фрагментов СС схожих с имеющимися, с учетом физико- географических условий местности и топологических неоднородностей, возникших в процессе развития сети, за счет того, что исходные данные для моделирования формируют исходя из топологической структуры реальной сети [2,3].

Алгоритм реализуемый данным способом предусматривает выполнение следующих действий:

– формирование исходных данных для моделирования, а именно: количество неоднородностей m, минимальное и максимальное количество элементов в неоднородностях Nmin, Nmax, минимальное и максимальное расстояние между центрами неоднородностей Lmin, Lmax, радиус неоднородности Rs.

– моделирование расположения неоднородностей в заданном фрагменте.

– моделирование элементов в каждой неоднородности. Формирование исходных данных для моделирования реализовано в виде алгоритма, представленного далее

Ввод исходных данных, а именно: площадь реального фрагмента сети связи выбранного региона, радиусы неоднородностей Rmin, Rmax, шаг изменения радиуса ΔR.

– нумерация от 1 до 7 элементов и СС заданного фрагмента.

– фиксация географических координат (Xi,Yi) элементов сети связи заданного фрагмента.

– фиксация географических областей, недоступных для связи в заданном фрагменте.

– выделение неоднородностей сети связи заданного фрагмента путем применения адаптированного алгоритма кластеризации FOREL.

Так как алгоритм вычисляет центры кластеров, то вычислительно более эффективными можно определить следующие функционал:

1. Сумма средних внутри кластерных расстояний должна быть меньше, где kc-центр кластера C.

2. Сумма межкластерных расстояний должна быть как можно больше, где k-центр тяжести всей выборки.

Выделение кластеров (неоднородностей) сети связи заданного фрагмента производится следующим образом:

1. задание радиуса кластера (неоднородности) Rs=Rmin. Выделение первого кластера (неоднородности).

2. совмещение центра кластера (неоднородности) с координатами первого элемента сети связи заданного фрагмента.

3. вычисление расстояния от центра кластера (неоднородности) до всех остальных элементов СС.

4. сравнение вычисленных расстояний с заданным радиусом кластера (неоднородности).

5. фиксация координат элементов сети связи, для которых rij<R.

6. вычисление координат центра тяжести для зафиксированных точек.

7. вычисление расстояния от центра тяжести до всех остальных элементов сети связи ρci.

8. сравнение вычисленных расстояний с заданным радиусом кластера (неоднородности).

9. фиксация координат точек, для которых расстояние меньше заданного радиуса кластера (неоднородности) ρci<Rs.

10. вычисление координат центра тяжести для зафиксированных точек.

11. проверка, на то совпали ли координаты центров тяжести. Если нет, то повторяют шаги, по определению центров тяжести, пока координаты центров тяжести не совпадут.

12. причисление элементов СС, расстояние до которых меньше заданного радиуса, к первому кластеру (неоднородности) С1. Фиксация результата.

13. исключение элементов СС, причисленных к первому кластеру (неоднородности), из множества.

14. проверка, все ли элементы СС причислены к кластерам (неоднородностям). Если нет, то приступают к выделению второго кластера (неоднородности), выбирая начальную точку из оставшегося множества. И так далее, пока все элементы не будут причислены к Cm кластерам (неоднородностям).

15. вычисление значения функционалов качества Ф0 и Ф1 по правилам (1) и (2).

16. запоминание значения функционалов качества, радиус кластера (неоднородности) Rs, количество кластеров (неоднородностей) m и их состав. Повторяют вышеперечисленные действия, начиная кластеризацию со второго элемента (i=2), потом с третьего(i=3), …до I-го (i=I).

17. увеличивают значение заданного радиуса кластера (неоднородности) на величину ΔR.

18. проверка, не достигло ли значение радиуса неоднородности максимального заданного Rmax.

Если увеличенное значение радиуса кластера (неоднородности) RS достигло максимального заданного значения Rmax, то выбирают вариант с наилучшими функционалами качества Ф0 и Ф1 при условии Ф0→min; Ф1→max, фиксируют радиус кластера (неоднородности) RS, количество m и состав кластеров (неоднородностей) для данного варианта.

1. исключение остальных ранее запомненных результатов итераций.

2. подсчет количества элементов в каждом кластере (неоднородности). Фиксация минимального Nmin, максимального Nmax количества элементов в кластерах (неоднородностях).

3. вычисление расстояния Lmk между центрами кластеров (неоднородностей). Фиксируют минимальное Lmin, максимальное Lmax расстояния между центрами кластеров (неоднородностей).

4. выведение всех необходимых для дальнейшего моделирования данных: количество неоднородностей m, минимальное, максимальное количество элементов в неоднородностях Nmin, Nmax, минимальное, максимальное расстояние между центрами неоднородностей Lmin, Lmax, радиус неоднородности Rs.

5. моделирование расположения неоднородностей в заданном фрагменте местности.

6. моделирование расположения элементов в каждой неоднородности с учетом физико-географических условий местности.

7. выбор первой сформированной топологической неоднородности m′ и вычисление количества элементов СС для данной неоднородности.

Если все координаты всех элементов неоднородности сформированы, то переходят к моделированию расположения элементов СС в следующей неоднородности. Проверка, во всех ли m неоднородностях смоделировано расположение элементов. Если нет, то повторяют действия, выполняемые для моделирования элементов первой неоднородности.

Заключение. Таким образом, применение рассмотренного способа моделирования системы связи позволит должностным лицам органов военного управления, повысить достоверность и адекватность моделирования, а также появляется возможность моделирования фрагментов сетей связи специального назначения.

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б. Я., Яковлев С. А. «Моделирование систем». – М.: Высшая школа, 2009, - 343 с.
2. Шелухин О. И., Тенякшев А. М., Осин А. В. «Моделирование информационных систем». Учебное пособие. – М.: Радиотехника, 2005. – 368 с.
3. Давыдов В. Н. «Сети электросвязи». – М.: Связь, 1977. – 366 с.
4. Агеев С.А., Бушуев А.С., Егоров Ю.П., Саенко И.Б. «Концепция автоматизации управления информационной безопасностью в защищенных мультисервисных сетях специального назначения // Автоматизация процессов управления». 2011. № 1. 50-57 с.

УДК: 004.056.53

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ПЕРЕДАЧИ, ХРАНЕНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ

Волостных Виктор Анатольевич, Рогов Руслан Александрович, Митрофанов Михаил Валерьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: rus6283@list.ru

Аннотация. В докладе рассмотрена необходимость проведения мероприятий защиты информации в системах передачи, хранения и обработки информации, а также основные причины, влекущие за собой утечку информации с данных систем.

Ключевые слова: *информационная безопасность; системы передачи; хранения и обработки информации; информация конфиденциального характера; утечка информации.*

PROTECTION OF INFORMATION IN THE SYSTEMS OF TRANSMISSION, STORAGE AND PROCESSING OF INFORMATION

Volostnykh Viktor, Rogov Ruslan, Mitrofanov Mikhail
Military Academy of communications
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: rus6283@list.ru

Abstract. The report considers the need to carry out information protection measures in information transmission, storage and processing systems, as well as the main reasons leading to information leakage from these systems.

Keywords: *information security; information transfer; storage and processing systems; confidential information; information leakage.*

Появление новых информационных технологий и развитие мощных компьютерных систем передачи, хранения и обработки информации повысили требования к уровню зашиты информации и вызвали необходимость, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Таким образом, средства обеспечения информационной безопасности стали одной из обязательных характеристик данных систем. На сегодняшний день существует широкий круг систем передачи, хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности, хранения конфиденциальной информации имеет особое значение [1, 2].

Актуальность применения данных систем связана с значительно упростившемся порядком работы, а также с сокращением времени обмена документами между пользователями системы. В связи с использованием в вышеперечисленных системах большого количества информации содержащей сведения государственной тайны или информации конфиденциального характера, в значительной степени привлекли к себе внимания злоумышленников, которые всевозможными способами пытаются завладеть, изменить или удалить данную информацию из системы. Таким образом, главной задачей защиты информации является изолирование нормально функционирующей информационной системы от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения [3].

Рассматривая угрозы безопасности систем передачи, хранения и обработки информации, их следует разделить на преднамеренные и случайные.

Исходя из публикаций последних лет в данной области, можно сделать вывод, что, как минимум, 70% утечки информации связанна с случайными (непреднамеренными) угрозами. При этом 95% снижения эффективность защиты связанно с самим пользователем. Простейшая не внимательность, безответственное отношение, а зачастую элементарное незнание использованиясистем передачи, хранения и обработки информации в комплексе.

Существуетсистемный подход к организации защиты информации от несанкционированного доступа. К методам и средствам зашиты информации относят организационные, техническиеи правовые [4, 5].

При это в данном подходе должным образом не уделяется внимание вопросам комплексной подготовки пользователей данной системы, проведение контрольных занятий, доведение статей, предусматривающих ответственность виновных утрате или утечки какой-либо информации, что является весомым аргументом в системе защиты информации.

Важно понимать, что основная утечка данных происходят не благодаря хитроумным способам, а из- за небрежности и невнимательности.

Исходя из этого можно сделать вывод, что, уделяя больше внимания комплексной подготовке пользователей систем передачи, хранения и обработки информации, соблюдения новых стандартов ФСТЭК, психосихо-эмоционального подбора личного состава можно не только снизить количество утечек информации, но и повысить эффективность функционирования самой системы.

СПИСОК ЛИТЕРАТУРЫ

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. 3-е изд., стер. - М.: Академия, 2008. - 336 с.
2. Черней Г.Л, Охрименко С. А., Ляху Ф. С. Безопасность автоматизированных информационных систем. Ruxancia, 1996. - 225 с.
3. Галатенко, ВЛ. Основы информационной безопасности.
4. Лепешкин О.М., Харечкин П. В. Функционально-ролевая модель управления доступом в социотехнических системах. Известия ЮФУ. Технические науки. 2009. № 11 (100). С. 52-57.
5. Бурлов В.Г., Лепешкин О.М.Методологический подход к оценке безопасности функционирования социальной и экономической системы управления регионаПроблемы экономики и управления в торговле и промышленности. 2013. № 2. С. 99-103.
6. Лепешкин О.М.Разработка подхода по оценке функциональной безопасности критической социотехнической системы. Инфокоммуникационные технологии. 2008. Т. 6. № 3. С. 113-116.

УДК 004

О НЕКОТОРЫХ МЕТОДАХ СЕТЕВОГО АНАЛИЗА

Гапочкин Артем Владимирович[1], Михайличенко Николай Валерьевич[2]
[1]Московский политехнический университет
Россия, Москва, ул. Большая Семеновская, 38
[2]Военная академия связи имени Маршала Советского Союза С.М.Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: Warrior_555@rambler.ru,23esn2008@rambler.ru

Аннотация. Сниффинг пакетов в сети без коммутаторов. Данные, полученные с помощи сниффера, могут быть использованы хакером для получения легального доступа к сервисам системы на правах законного пользователя. В докладе рассматриваются существующие 3 меры противодействия данному виду атак на основе сканирования сети. До выполнения активных атак злоумышленнику необходимо узнать всю информацию о самой структуре сети и сервисах. В статье моделируется с помощью сети Петри-Маркова процесс сканирования сети.

Ключевые слова: *сниффинг; сетевой анализ; сеть Петри-Маркова.*

SOME METHODS OF NETWORK ANALYSIS

Gapochkin Artem[1],Mikhaylichenko Nikolay[2]
[1]Moscow Polytechnic University, Russia, Moscow, Bolshaya Semenovskaya, 38
[2]Military Academy of communications named after Marshal of the Soviet Union S. M. Budyonny"
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: Warrior_555@rambler.ru, 23esn2008@rambler.ru

Abstract. Sniffing of packages in network without switchboards. The data received from the help of a sniffer can be used by the hacker for receiving legal access to services of system as the lawful user. In the report the existing 3 measures of counteraction to this type of the attacks on the basis of scanning of network are considered. Before performance of the active attacks the malefactor needs to find all information on the structure of network and services. In article process of scanning of network is modelled by means of Petri-Markov's network.

Keywords: *sniffing; network analysis; Petri net and Markov.*

Активной называется такая атака, при которой оппонент имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения. Пассивной называется такая атака, при которой оппонент не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Она является подготовительным этапом при реализации многих активных сетевых атак. Когда вместо коммутаторов в сети установлены концентраторы, то пакеты, полученные рассылаются всем компьютерам в сети, и только после этого компьютеры определяют для кого этот пакет [1]. Целью пассивной атаки может быть только прослушивание передаваемых сообщений и анализ трафика.

Если хакер получит доступ к такой сети или непосредственно к компьютеру, то ему станет доступна вся передаваемая информация в сети, он может также перехватывать пакеты, если вставит сетевую карту в режим прослушивания. Несанкционированное прослушивание и наблюдение за данными сети, с помощью которых хакер получает легальный доступ к сервисам системы на правах законного пользователя, производится с помощи специальной программы - пакетного сниффер.

В данном примере сети позиции не имеют инцидентные дуги, следовательно, вероятности перемещения из них в переходы равны единице.

Полушаг из перехода в позицию срабатывает мгновенно и динамика срабатывания сети может определяться только вероятностями перемещений этой сети, а также плотностями распределения времени нахождения процесса в каждом из процессов. Следовательно, в сети необходимо рассмотреть только процесс перехода из s1 (начального состояния) в t2 (конечный переход) [2].

До выполнения активных атак злоумышленнику необходимо узнать всю информацию о самой структуре сети и сервисах. Смоделируем с помощью сети Петри-Маркова сканирование сети. После настройки параметров, осуществляется посылка ICMP- эхо - запросов, хостов, IP-адресов в режиме многопоточном. Путем посылки нестандартных пакетов, злоумышленник может определить тип ОС, однако стандарты упускают реакцию на недопустимые входные данные. Следовательно, индивидуальные реакции каждой определенной ОС на нестандартные пакеты формируют сигнатуру, по которой злоумышленник может определить под каким управлением работает данный компьютер. В случае, если хост определен как активный, то определяется наличие работающего сервиса. Результатом данной проверки является выявление наиболее уязвимых компьютеров. Смоделируем данную атаку с помощью модели Петри-Маркова.

В докладе рассмотрены способы моделирования процессов сетевого анализа при угрозах доступа к элементам ИТКС. Данные методы являются подготовительными этапами для проведения активных атак злоумышленниками. Моделирование этих процессов может позволить более детально проанализировать отдельные стадии атак на сеть и эффективно предотвращать активные атаки на стадии их подготовки.

СПИСОК ЛИТЕРАТУРЫ

1. Радько Н.М. Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. РадиСофт, 2010 – 232с. С.122-127.
2. Закалкин П.В., Сагдеев А.К., Стародубцев Ю.И., Сухорукова Е.В. Проблема формирования системы динамической защиты государственных информационных систем. / Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т./ под ред. С.В. Бачевского, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. – СПб.: Санкт-Петербургский университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2016. – 550 с. С. 239-243.
3. Саенко И.Б., Бирюков М.А. Методика интеграции локальных схем разграничения доступа к разнородным ресурсам единого информационного пространства // Информационные технологии в управлении (ИТУ-2016) Материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В.Г. Пешехонов. 2016. С. 758-762.

УДК 004.056.57

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Гладков Владимир Владиславович, Тараскина Анастасия Геннадьевна,
Кузнецов Сергей Иванович, Тесля Сергей Петрович, Акишин Андрей Владимирович
Военная академия связи имени Маршала Советского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: akishin1977@mail.ru

Аннотация. В работе рассматриваются методы построения систем обнаружения DDoS-атак на основе нейронных сетей и их эффективность.

Ключевые слова: *искусственнаянейронная сеть; DDoS-атака; сетевая атака; информационная угроза; альтернативные методы.*

THE USE OF NEURAL NETWORKS TO DETECT NETWORKS ATTACKS

Gladkov Vladimir, Taraskina Anastasiya, Kyznecov Sergey, Tesla Sergey, Akishin Andrey
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckystr., 3
e-mail: akishin1977@mail.ru

Abstract. In the paper method of construction of system of detection of DDoS-attacks on the basic of neural networks and their efficiency.

Keywords: *artificial of neural networks; DDoS-attack; network attack; alternative methods.*

В последнее время в разных отраслях науки и техники отмечается интерес к применению искусственных нейронных сетей. Популярность нейронных сетей объясняется возможностью их эффективного использования в задачах плохо решаемых "аналитическими" методами. В теоретических работах [1, 2, 3, 4], посвященных нейронным сетям отмечается целесообразность их использования в задачах: классификации образцов, кластеризации/категоризации, аппроксимации функций, предсказания/прогноза, создания информационно-вычислительных систем, обладающих памятью, адресуемой по содержанию, т.е. ассоциативной.

Отметим, что частично или в комплексе, решать перечисленные задачи приходиться при разработке методов и средств защиты информации.

Среди множества видов сетевых атак наибольшее распространение получила атака типа DDoS. По данным статистики данный вид угрозы занимает одно из лидирующих мест ежегодно. Причинами распространения подобного вредоносного сетевого воздействия является простота реализации, исчерпывающие сведения о механизме исполнения и малые требования к знаниям и вычислительным ресурсам злоумышленника.

Практически все современные программные и программно-аппаратные средства защиты для успешного противодействия сетевым атакам используют целый набор методов и механизмов противодействия DDoS-атакам. Основные механизмы, применяемые в современных средствах противодействия DDoS-атакам, представлены в статье Частикова В.А. [5]. Бесплатная защита от DDoS-атак перешла в число представителей «вымирающего вида». Эффективные средства стоят немало денег. Некоторые методы и механизмы противодействия DDoS-атакам очень дороги и не очень эффективны, другие достаточно эффективны и доступны по цене не всем, но бесплатных нет.

Как следствие одним из недостатков применения современных программных и программно-аппаратных средства защиты является их высокая стоимость и как следствие отказ от их приобретения и эксплуатации, что приводит к существенному росту финансовых и клиентских потерь при осуществлении сетевых атак.

Анализ исследований и разработок, проводимых в настоящее время в этом направлении, показал, что достижение соответствующих уровней защиты системы от DDoS-атак невозможно на основе применения обычных алгоритмических и программно-аппаратных решений.

Современные средства обнаружения DDoS-атак неизбежно должны включать в себя интеллектуальные подсистемы, по крайней мере, в качестве одной из своих составных частей. По этой причине способы и средства обнаружения DDoS-атак должны постоянно исследоваться и совершенствоваться.

Разработки в области применения нейронных сетей известных отечественных и зарубежных исследований показали эффективность применения нейронной сети для системы обнаружения DDoS-атак на основе применения различных схем их реализации. Их эффективность превосходит существующие решения на 15%.

Преимуществом систем обнаружения DDoS-атак на основе нейронных сетей является: гибкость, которая выражается в способности обрабатывать данные из нескольких источников в нелинейной форме; высокая скорость обработки информации нейронной сетью, как следствие высокая реакция на вторжение до того, как будет нанесен непоправимый ущерб системе; возможность прогнозирования обнаружения случаев DDoS-атак, по мере получения опыта, как следствие отслеживания последующего возникновения этих событий; способность нейронной сети "обучаться" признакам DDoS-атак и определять случаи, которые нехарактерны для тех, что наблюдались ранее.

Применение нейронных сетей для обнаружения сетевых атак является одним из наиболее эффективных и перспективных методов обнаружения DDoS-атак.

Несмотря на преимущества системы обнаружения атак на основе нейронных сетей они обладают недостатками, к которым можно отнести:

– требованиями к обучению нейронной сети (т.к. способность искусственной нейронной сети к идентификации признаков вторжение полностью зависит от правильного обучения системы);

– решение задач получения представительной статистики и ее нормализации, объединения вычислительных ресурсов;

– требования к большим вычислительным мощностям;

– невозможность оперативного анализа больших объемов данных в условиях работы в качестве сетевой системы обнаружения вторжений большой сети.

Потенциальная реализация предполагает включение систем обнаружения DDoS-атак на основе нейронных сетей в существующие или определяет нейронную сеть как автономную систему обнаружения DDoS-атак. В отличие от первого подхода, использование нейронной сети как автономной системы обнаружения DDoS-атак дает более широкие возможности.

Современный подход к построению систем обнаружения DDoS-атак на информационные системы полон недостатков и уязвимостей, позволяющих, к сожалению, злонамеренным воздействиям успешно преодолевать системы защиты информации. Переход от поиска сигнатур атак к выявлению предпосылок возникновения угроз информационной безопасности должен способствовать тому, чтобы в корне изменить данную ситуацию, сократив дистанцию отставания в развитии систем защиты от систем их преодоления.

Рассмотренные работы позволяют сделать выводы об эффективности применения нейронных сетей для системы обнаружения DDoS-атак. Нейронные сети создают платформу для дальнейшего изучения и проектирования альтернативных методов анализа сетевых аномалий и поиска сетевых вторжений.

СПИСОК ЛИТЕРАТУРЫ

1. Ежов А.А., Шумский С.А. Нейрокомпьютинг и его применения в экономике и бизнесе. – М.: МИФИ, 1998. – 224 с.
2. Круглов В.В., Борисов В.В. Искусственные нейронные сети. – М.: Горячая линия-Телеком, 2002. – 382 с.
3. Каллан Р. Основные концепции нейронных сетей. : Пер. с англ. – М.: Вильямс, 2003. – 288 с.
4. Люгер Ф. Искусственный интелект: стратегии и методы решения сложных проблем, 4-е издание.:
1. Пер. с англ. – М.: Вильямс, 2003. – 864 с.
5. Частикова В.А., Картамышев Д.А., Власов К.А. НЕЙРОСЕТЕВОЙ МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ ОТ DDOS-АТАК //
2. Современные проблемы науки и образования. – 2015. – № 1-1.; URL : https://science-education.ru/ru/article/view?id=18343
3. (дата обращения: 13.09.2017).

УДК 681.5.015

ВОПРОСЫ ПЛАНИРОВАНИЯ МЕРОПРИЯТИЙ ОПЕРАТИВНО-ТЕХНИЧЕСКОЙ СЛУЖБЫ НА ОБЪЕКТАХ АВТОМАТИЗАЦИИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Григорян Вазген Мкртичевич, Куликов Владимир Алексеевич
Пантюхин Олег Игоревич, Солодухин Борис Владимирович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: p_oleg99@mail.ru

Аннотация. В работе рассмотрены вопросы планирования мероприятий оперативно-технической службы на объектах автоматизации специального назначения. Одним из основных подходов к автоматизации планирования является применение методов, разработанных на основе моделей сетевого планирования и управления. Показаны преимущества моделей и полезность применения соответствующих программных средств.

Ключевые слова: *оперативно-техническая служба; сетевое планирование и управление; программные средства.*

THE EVENTS PLANNING OF THE OPERATIONAL-TECHNICAL SERVICES FOR FACILITIES AUTOMATION SPECIAL PURPOSE

Grigoryan Vazgen, Kulikov Vladimir, Pantyukhin Oleg, Solodukhin Boris
Millitary Academy of Communications named S.M. Budyonnogo.
Russia, St. Peterburg, Tikhoretsky pr., 3
e-mail: p_oleg99@mail.ru

Abstract. The paper considers the questions of planning of the operational-technical services on automation objects for special purposes. One of the main approaches to automated planning is the application of methods developed on the basis of models of network planning and management. Advantages of the models and the usefulness of the relevant software.

Keywords: *operational-technical service; network planning and management; software tools.*

Сокращение времени на принятие решения и его обоснование являются предпосылками необходимости автоматизации процессов планирования мероприятий оперативно-технической службы (ОТС) на объектах автоматизации (ОА) специального назначения. Постоянная готовность автоматизированных систем управления к использованию по назначению и эффективность их применения достигается правильной организацией мероприятий ОТС на объектах автоматизации.

В процессе планирования мероприятий необходимо учитывать сложность получения всех исходных данных для организации ОТС за ограниченный период времени, перемещение мобильных ОА при изменении обстановки по связи и автоматизации, что вызывает необходимость разработки (уточнения) документов по ОТС в новых районах их размещения. В настоящее время одним из основных подходов к автоматизации планирования является применение методов, разработанных на основе моделей сетевого планирования и управления (СПУ). СПУ – это система планирования и управления различных процессов, основанная на использовании сетевых моделей, в частности сетевых графов, позволяющая определить оптимальную последовательность планируемых работ и их взаимосвязь [1].

Цель метода сетевого планирования – спланировать, организовать и произвести комплекс работ в полном объеме и с высоким качеством в заданное время. Его применение для автоматизации разработки документов по ОТС позволит:

– оптимальным образом выполнить весь комплекс работ, возлагаемых на систему планирования ОТС объекта автоматизации;

– скоординировать работу должностных лиц и обеспечить высокую наглядность хода выполнения работ, проводимых в системе управления и планирования мероприятий ОТС;

– иметь возможность в случае необходимости, перераспределять людские ресурсы между работами.

Методы СПУ необходимо активно использовать для планирования мероприятий ОТС. Это обусловлено: наличием взаимосвязанных работ при разработке документов группой исполнителей; ограниченным временем на выполнение работ; ограничениями на все виды ресурсов.

В настоящее время на рынке программных продуктов имеются различные программные средства, реализующие сетевые методы планирования: от мощных профессиональных систем до систем, позволяющих эффективно распорядиться рабочим временем, финансовыми средствами и т.п. Одним из современных средств СПУ выступает Microsoft Project.

Microsoft Project позволяет представить информацию о работах проектов в формах PERT, GANTT, календаря, позволяющих отобразить работы плана на одном-двух уровнях иерархии. Для каждой работы на данных диаграммах указываются длительность, сроки начала и конца, множество

непосредственно предшествующих работ, исполнители, а также другие характеристики. Пользователю дополнительно предоставляются широкие возможности самому выбирать форму диаграмм и совмещать их на экране монитора [2,3].

Заключение. В настоящее время должностные лица, отвечающие за планирование и контроль мероприятий ОТС, в большинстве не используют программные средства сетевого планирования, предпочитая им исполнение документов в графических и текстовых редакторах. Это неизбежно приводит к увеличению сроков разработки планов мероприятий ОТС на объектах автоматизации. Безусловно, нужно учитывать, что использование средств сетевого планирования целесообразно начинать с уровней управления имеющих значительный объем задач, оперирующих распределением ресурсов и обладающих малыми сроками на исполнение планов и их оперативную корректировку. Целесообразность использования средств сетевого планирования, подтверждена во всем мире и, несомненно, что вопрос внедрения средств и методов сетевого планирования в системах специального назначения только вопрос времени.

СПИСОК ЛИТЕРАТУРЫ

1. Анфилатов В.С., Авраменко В.С., Пантюхин О.И. Теоретические основы автоматизации управления войсками и связью. Часть 2. Основы построения и функционирования систем автоматизации управления войсками и связью: Учеб. пособие. – СПб.: ВАС, 2015г. – 304с.
2. Григорян В.М., Куликов В.А., Куликов А.В.Проблемыпланированиямероприятийоперативно-технической службына объектах автоматизации сетей связиспециального назначения. /Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI международная НТ и НМ конференция: сб.науч.ст.в 4т. СПб.: СПбГУТ, 2017. Т.2. 580с.
3. Агеев С.А., Бушуев А.С., Егоров Ю.П., Саенко И.Б. Концепция автоматизации управления информационной безопасностью в защищенных мультисервисных сетях специального назначения // Автоматизация процессов управления. 2011. № 1. С. 50-57

УДК 621.004

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПОД УПРАВЛЕНИЕМ ОПЕРАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ASTRA LINUX SE

Гринь Дарья Владимировна[1], Ильина Ольга Борисовна[1], Купчиненко Ольга Павловна[1], Скоропад Александр Витальевич[2]
[1]Военная академия связи имени Маршала Советского Союза С. М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
[2]Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио» (Филиал ФГУП НИИР-ЛОНИИР)
Россия, Санкт-Петербург, Большой Смоленский пр., 4
e-mails: voca_g@mail.ru, nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Аннотация. Проведен анализ комплекса средств защиты информации от несанкционированного доступа в операционной системе специального назначения AstraLinuxSE. Проанализированы вопросы применение базовых и дополнительных средств защиты информации в операционной системе AstraLinuxSE.

Ключевые слова: *автоматизированная система; защита информации; несанкционированный доступ; модели разграничения доступа.*

THE PROTECTION OF INFORMATION FROM UNAUTHORIZED ACCESS IN AUTOMATED SYSTEMS UNDER THE MANAGEMENT OF THE SPECIAL EDITION OPERATIONAL SYSTEM ASTRA LINUX SE

Grin Daria[1], Ilina Olga[1], KupchinenkoOlga[1], Skoropad Aleksandr[2]
[1]Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
[2]Radio Research & Development Institute «Leningrad Branch of Radio Research & Development Institute» (Branch NIIR-LONIIR)
Russia, St. Petersburg, Bolshoy Smolensky pr., 3
e-mails: voca_g@mail.ru, nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Abstract. The analysis of the complex of information protection against unauthorized access have done in the Astra Linux SE OS. The questions of using basic and additional means of information protection in the Astra Linux SE OS are analyzed.

Keywords: *automation system; protection of information; unauthorized access; models of access control.*

Функционал операционной системы (ОС) Astra Linux SE расширен комплексом средств защиты (КСЗ) от несанкционированного доступа (НСД), реализующим дополнительные функции администрирования ОС, которая работает в составе автоматизированных систем (АС) в защищенном

исполнении. Ряд средств КСЗ являются базовыми – встроенными в функционал ОС Debian GNU Linux, на основе которой разработана ОС Astra Linux SE.

В многопользовательских ОС реализованы следующие механизмы разграничения доступа [1]:

– децентрализованные механизмы предполагают наличие для каждого объекта (например, файла или директории) его владельца, который задает правила назначения прав доступа к этому объекту индивидуально (дискреционная модель разграничения доступа).

– централизованные механизмы предполагают администрирование правил назначения доступа к объектам, специально выделенным лицом (мандатная модель разграничения доступа).

Использование того или иного класса механизмов зависит от функционального предназначения ОС. В ОС Astra Linux SE механизм разграничения доступа является комбинированным и поддерживает, как дискреционную, так и мандатную модель разграничения доступа.

Отдельным классом задач, решаемым администратором ОС Astra Linux SE являются задачи администрирования при эксплуатации этой ОС в качестве основы АС в защищенном исполнении.

Для решения этих задач базовый комплекс средств администрирования дополнен КСЗ подсистема безопасности PARSEC.

Подсистема безопасности PARSEC интегрирована с базовым комплексом средств администрирования ОС Astra Linux SE. Средства, входящие в состав подсистемы PARSEC, служат для решения задач, связанных как с формированием новых, так и с эксплуатацией имеющихся АС в защищенном исполнении на базе ОС Astra Linux SE.

Поскольку ОС Astra Linux SE является POSIX-совместимой системой, то в качестве реализации дискреционной модели разграничения доступа в ней используется стандарт POSIX ACL (Access Control Lists – списки контроля доступа).

Кроме этого стандарта, поддерживаемого большинством UNIX-совместимых систем, ОС Astra Linux SE поддерживает стандарт ACL, специфичный для объектов файловой системы extfs.

Благодаря этому, файл, созданный в ОС Astra Linux SE, не потеряет разрешения на доступ, будучи скопирован, например, в файловую систему любой из версий ОС UNIX или других дистрибутивов ОС Linux.

Механизм разрешений на доступ POSIX ACL поддерживается на уровне архитектуры файловой системы ОС Astra Linux SE, путем включения стандартных (Minimal ACL) и расширенных (Extended ACL) атрибутов доступа в inode каждого файла и директории.

Атрибуты Minimal ACL поддерживает три базовых класса субъектов доступа к файлу:

1. User access (u) – доступ для владельца файла;
2. Group access (g) – доступ для группы, владеющей файлом;
3. Other access (o) – доступ для остальных пользователей (кроме пользователя root).

Применительно к КСЗ ОС Astra Linux SE эта схема расширена и основывается на использовании механизма PAM (Pluggable Authentication Modules – подключаемые модули аутентификации).

Механизм PAM - набор разделяемых библиотек (расположение /lib/security), с помощью которых администратор ОС Astra Linux SE может организовать процедуру аутентификации (подтверждение подлинности) пользователей запускаемыми программами. Каждый модуль реализует собственный механизм аутентификации. Изменяя набор и порядок следования модулей PAM, возможно создать уникальный сценарий аутентификации.

Подобный подход позволяет динамически изменять процедуру аутентификации без внесения изменений в исходный код ядра ОС Astra Linux SE.

Наиболее распространенным вариантом модели мандатного разграничения доступа является модель «контекст-тип». Согласно этой модели, любой процесс запускается в поименованном контексте безопасности, а каждый объект доступа имеет определённый тип (уровень секретности).

Одним из вариантов такой модели является многоуровневая иерархическая система доступа (MLS, Multilevel security). В этой модели уровни доступа (контексты безопасности) и уровни секретности (типы) ранжированы. Основным правилом является запрет на операцию чтения из объектов более высокого уровня секретности и операцию записи в объекты с более низким уровнем секретности.

Модель мандатного разграничения доступа в ОС Astra Linux SE является вариантом реализации модели MLS.

Ее основой является следующий факт - решение о запрете или разрешении доступа субъекта к объекту принимается комплексно на основе:

– контекста безопасности субъекта;

– метки безопасности объекта;

– типа операции доступа: Чтение, Запись, Исполнение (rwx) – модель дискреционного разграничения доступа [2].

При создании субъектом любого из объектов доступа подсистем ОС Astra Linux SE, этот объект доступа наследует метку безопасности на основе контекста безопасности процесса. При этом тип

метки безопасности устанавливается равным нулю. Реализация модели мандатного разграничения доступа затрагивает все подсистемы ядра, в которых реализована модель дискреционного разграничения доступа.

Доступ разрешается в том случае, если он возможен относительно дискреционных и мандатных правил разграничения доступа и запрещается в случае, если доступ запрещен относительно любой из этих моделей.

Заключение. Модели дискреционного и мандатного разграничений доступа реализованы в ядре ОС Astra Linux SE, что обеспечивает их правильное функционирование при выполнении любых функций, предоставляемых ОС Astra Linux SE. Кроме того, обе модели разграничения доступа функционируют параллельно, не влияя на принятие взаимных решений (обеспечивается непротиворечивость функции разграничения доступа). Применение базовых и дополнительных КСЗ в ОС Astra Linux SE позволяют построить гибкую, надежную и многофункциональную систему защиты информации от НСД.

СПИСОК ЛИТЕРАТУРЫ

1. Новые информационные и сетевые технологии в системах управления военного назначения. Часть 2. Новые сетевые технологии в системах военного назначения. Учебник. Под редакцией профессора И.Б.Саенко. – СПб: ВАС, 2010, С. 416-420.
2. Система обмена информацией в электронном виде Вооруженных сил Российской Федерации. Часть 1. Общие положения по построению системы обмена информации в электронном виде Вооруженных сил Российской Федерации. Учебное пособие. Под редакцией О.В. Рисмана. – СПб.: ВАС, 2011, С. 202-205.

УДК 681.5.015

К ВОПРОСУ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПЛАНИРОВАНИЯ ПОВСЕДНЕВНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНА УПРАВЛЕНИЯ

Гурьев Сергей Николаевич, Щербаков Александр Юрьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: iapbgks@bk.ru

Аннотация. В докладе рассматриваются вопросы повышения эффективности планирования управленческой деятельности, позволяющих повысить оперативность разработки служебных документов, автоматизировать процессы нетворческого характера, осуществлять контроль документооборота, проводить анализ уже выполненных мероприятий, а также создать базу стандартных формализованных документов, что в целом повысит эффективность управленческой деятельности.

Ключевые слова: *управление, средства автоматизации, программное обеспечение, планирование, повседневная деятельность, управленческая деятельность, эффективность*.

TO THE QUESTION OF IMPROVING THE EFFICIENCY OF THE EVERYDAY ACTIVITY OF THE GOVERNING BODY

Guryev Sergei, Scherbakov Aleksandr
Millitary Academy of Communications named S.M. Budyonnogo
Russia, St. Peterburg, Tikhoretsky pr., 3
e-mail: iapbgks@bk.ru

Abstract. In the report questions of increase in efficiency of planning of administrative activity, the in-house documents, to automate processes of not creative character, to exercise document flow control, to carry out the analysis of already executed actions and also to create base of the standard formalized documents that in general will increase efficiency of administrative activity allowing to increase efficiency of development are considered.

Keywords: *management; automation tools; software planning; daily activities; management activities; efficiency.*

Один из подходов к определению понятия управления говорит о том, что Управление -это процесс управленческой деятельности, т.е. совокупность выполняемых в определенной последовательности действий субъекта управления по выработке и осуществлению управляющего воздействия на объект управления для достижения определенной цели.

При этом субъектом управления может выступать орган управления, наделенный властными полномочиями по принятию решений, осуществлению управленческих функций и воздействий в виде руководящих документов, которые доводятся объектам управления и подлежат учету, контролю и оперативному регулированию.

Существующая в настоящее время методология описания моделирования процессов управленческой деятельности в области автоматизированных систем специального назначения позволяет формализовать процессы управленческой деятельности ДЛ ОУ, повысить эффективность функционирования подсистемы планирования в условиях повседневной деятельности.

В настоящее время для реализации автоматизации планирования повседневной деятельности органов управления применяются автоматизированные рабочие места из состава комплексов средств автоматизации, программное обеспечение, общесистемное программное обеспечение (ОСПО), специальное программное обеспечение(СПО), документальные базы данных(ДБД).

Современные информационные и сетевые технологии предоставляют должностным лицам (ДЛ) ОУ весь спектр услуг связи, а технические средства передачи данных позволяют получать удаленный доступ к совместно используемым ДБД (связаться по электронной почте, принимать участие в видеоконференции), повышая эффективность управления за счетсокращения времени цикла управления.

Заключение. Обобщая вышеизложенное, можно сделать вывод, что использование СПО в процессе планирования повседневной деятельности позволит повысить оперативность разработки служебных документов, за счет автоматизации процессов нетворческого характера, предоставит возможность осуществлять контроль их ведения, проводить анализ уже выполненных мероприятий, а также создать базу стандартных формализованных документов, (которая будет использоваться в дальнейшем при планировании повседневной деятельности), что в целом повысит эффективность управленческой деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Анфилатов В.С., Авраменко В.С., Пантюхин О.И. Теоретические основы автоматизации управления войсками и связью. Часть 2. Основы построения и функционирования систем автоматизации управления войсками и связью: Учеб. пособие. – СПб.: ВАС, 2015г. – 304с.
2. Черняков С.Б. Теория военного управления. Военная академия связи. 2015 г.
3. Авраменко В.С. Адаптивный контроль защищенности информации от несанкционированного доступа // Информация и космос. 2010. № 3. С. 116-119.

УДК 003.26

АБСОЛЮТНО СТОЙКОЕ КВАНТОВОЕ ШИФРОВАНИЕ

Гущин Игорь Николаевич, Петренко Михаил Игоревич, Овчинников Николай Юрьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: flanger1993@yandex.ru

Аннотация. Квантовая криптография по праву считается новым витком в эволюции информационной защиты. Именно она позволяет создать практически абсолютную защиту шифрованных данных от взлома.

Ключевые слова: *квантовая криптография; стойкое квантовое шифрование; криптография мобильных устройств; квантовое распределение ключей.*

ABSOLUTELY STANDBY QUANTUM ENCRYPTION

Gushchin Igor, Petrenko Mikhail, Ovchinnikov Nikolay
The S.M. Budjonny Military Academy of the Signal Corps
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: flanger1993@yandex.ru.ru

Abstract. Quantum cryptography is rightfully considered a new round in the evolution of information protection. It allows creating almost absolute protection of encrypted data from hacking.

Keywords: *quantum cryptography; persistent quantum encryption; cryptography of mobile devices; quantum key distribution.*

В основе устройства квантового шифрования лежат пространственные модуляторы света (SLM) — матрицы, преобразующие фазу и интенсивность проходящего сквозь них света определенным известным образом в зависимости от положения матрицы. Затем прошедший свет передается напрямую, открытым способом. При этом происходит линейный сдвиг точки фокуса луча. Не зная, какие именно преобразования были сделаны, невозможно восстановить исходные характеристики света.

Для расшифровки также используется модулятор света, выполняющий обратное преобразование. После этого свет фокусируется на однофотонный детектор 8×8 пикселей — положение точки фокуса соответствует записанной в фотонах информации. Таким образом, используя единичные фотоны для передачи данных, возможна передача до шести бит (26=8×8) информации на фотон [1].

Даже если перехватывающий открытую информацию злоумышленник будет обладать таким же модулятором света, каким обладают отправитель и получатель сигнала, не зная последовательность действий с модулятором, он не сможет восстановить информацию.

Ячейки Покеля необходимы для импульсной вариации поляризации потока квантов передатчиком и для анализа импульсов поляризации приемником. Передатчик может формировать одно из четырех состояний поляризации. Передаваемые данные поступают в виде управляющих сигналов на эти ячейки. В качестве канала передачи данных может быть использовано оптоволокно. В качестве первичного источника света можно использовать и лазер.

На принимающей стороне после ячейки Покеля установлена кальцитовая призма, которая расщепляет пучок на два фотодетектора (ФЭУ), измеряющие две ортогональные составляющие поляризации. При формировании передаваемых импульсов квантов возникает проблема их интенсивности, которую необходимо решать. Если квантов в импульсе 1000, есть вероятность, что 100 квантов по пути будет отведено злоумышленником на свой приемник. В последующем, анализируя открытые переговоры между передающей и принимающей стороной, он может получить нужную ему информацию. Поэтому в идеале число квантов в импульсе должно быть около одного. В этом случае любая попытка отвода части квантов злоумышленником приведет к существенному изменению всей системы в целом и, как следствие, росту числа ошибок у принимающей стороны. В подобной ситуации принятые данные должны быть отброшены, а попытка передачи повторена. Но, делая канал более устойчивым к перехвату, специалисты сталкиваются с проблемой “темнового” шума (получение сигнала, который не был отправлен передающей стороной, принимающей стороной) приемника, чувствительность которого повышена до максимума. Для того, чтобы обеспечить надежную передачу данных, логическому нулю и единице могут соответствовать определенные последовательности состояний, допускающие коррекцию одинарных и даже кратных ошибок.

Дальнейшего повышения отказоустойчивости квантовой криптосистемы можно достичь, используя эффект EPR, который возникает, когда сферически симметричный атом излучает два фотона в противоположных направлениях в сторону двух наблюдателей. Фотоны излучаются с неопределенной поляризацией, но в силу симметрии их поляризации всегда противоположны. Важной особенностью этого эффекта является то, что поляризация фотонов становится известной только после измерения. Экерт предложил криптосхему на основе эффекта EPR, которая гарантирует безопасность пересылки и хранения ключа. Отправитель генерирует некоторое количество EPR фотонных пар. Один фотон из каждой пары он оставляет для себя, второй посылает своему партнеру. При этом, если эффективность регистрации близка к единице, при получении отправителем значения поляризации 1, его партнер зарегистрирует значение 0 и наоборот. Таким образом партнеры всякий раз, когда требуется, могут получить идентичные псевдослучайные кодовые последовательности. Практически реализация данной схемы проблематична из-за низкой эффективности регистрации и измерения поляризации одиночного фотона.

Квантовая криптография еще не вышла на уровень практического использования [2], но приблизилась к нему. Конечно же, квантовое направление криптографической защиты информации очень перспективно, так как квантовые законы позволяют вывести методы защиты информации на качественно новый уровень. На сегодняшний день уже существует опыт по созданию и апробированию компьютерной сети, защищенной квантово-криптографическими методами – единственной в мире сети, которую невозможно взломать.

Квантовая криптография [3] — чрезвычайно надежный в теории метод защиты каналов связи от подслушивания, однако на практике реализовать его пока довольно трудно. На обоих концах канала должна быть установлена сложная аппаратура —источники одиночных фотонов, средства управления поляризацией фотонов и чувствительные детекторы. При этом для измерения угла поляризации фотонов необходимо точно знать, как ориентировано оборудование на обоих концах канала. Из-за этого квантовая криптография не подходит для мобильных устройств.

Ученые из Бристольского университета предложили схему, при которой сложное оборудование необходимо только одному участнику переговоров. Второй лишь модифицирует состояние фотонов, кодируя этим информацию, и отправляет их обратно. Аппаратуру для этого можно разместить в карманном устройстве. Авторы предлагают и решение проблемы ориентации оборудования. Измерения производятся в случайных направлениях. Список направлений может быть опубликован открыто, но при расшифровке будут учитываться только совпадающие направления. Авторы называют метод «независимым от системы отсчета квантовым распределением ключей».

СПИСОК ЛИТЕРАТУРЫ

1. А. Корольков, Квантовая криптография, или как свет формирует ключи шифрования, 1999.
2. В. Красавин, Квантовая криптография, 2010, 376с.
3. A.K. Ekert,”Quantum Cryptography Based on Bell’s Theorem”, Phys. Rev. lett. 67,661 (1991).

УДК621.391(075.8)

НЕКОТОРЫЕ ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ВЗАИМОДЕЙСТВИИ РЕГИОНАЛЬНЫХ КОРПОРАТИВНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ С СЕТЬЮ ОБЩЕГО ПОЛЬЗОВАНИЯ

Дедюрин Антон Борисович[1], Еричев Павел Сергеевич[1], Паращук Игорь Борисович[2]
[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mails: shchuk@rambler.ru,antd142@mail.ru

Аннотация. В материале рассмотрены современные тенденции и ключевые особенности функционирования системы защиты информации при взаимодействии региональных корпоративных телекоммуникационных сетей с сетью общего пользования (сетью Интернет), включая перечень защищаемых объектов, определяемый возможностями потенциального нарушителя по несанкционированному вмешательству. Предложена трактовка понятия и сущности современной системы защиты, предназначенной для реализации политики безопасности при взаимодействии телекоммуникационной сети с глобальной сетью Интернет.

Ключевые слова: *региональная телекоммуникационная сеть; защита информации; доступ; данные; система.*

SOME FEATURES OF THE FUNCTIONING OF INFORMATION SECURITY SYSTEM UNDER INTERACTION OF REGIONAL CORPORATE TELECOMMUNICATION NETWORKS WITH A COMMON USE NETWORK

Dediourin Anton[1], Yerichev Pavel[1], Parashchuk Igor[2]
[1]Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
[2] St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
e-mails: shchuk@rambler.ru, antd142@mail.ru

Abstract. The article considers modern trends and key features of the information security system functioning in the interaction of regional corporate telecommunication networks with the public network (Internet), including the list of protected objects, determined by the potential violator's capabilities for unauthorized interference. The interpretation of the concept and essence of the modern protection system intended for the implementation of the security policy in the interaction of the telecommunications network with the global Internet network is proposed.

Keywords: *regional telecommunications network; data protection; access; data; system.*

Широкое использование информационных технологий, с привлечением информационных ресурсов глобальной сети Интернет во всех сферах жизнедеятельности организаций и предприятий страны, делает весьма актуальной проблему защиты информации, ее пользователей, информационных ресурсов и каналов передачи данных от злоумышленников.

Специалист в области безопасности информации региональных корпоративных телекоммуникационных сетей (РКТС) отвечает за разработку, реализацию и эксплуатацию системы обеспечения информационной безопасности, направленной на поддержание целостности, пригодности и конфиденциальности данных, накопленных, хранимых и передаваемых по каналам РКТС. В его функции входит обеспечение физической (технические средства, линии связи и удаленные компьютеры) и логической (сами данные, прикладные программы, операционная система) защиты информационных ресурсов.

При взаимодействии РКТС с глобальной сетью Интернет ряд объектов телекоммуникационной сети могут подвергаться угрозам с точки зрения информационной безопасности: собственно информация; оборудование и элементы инфраструктуры РКТС; программное обеспечение РКТС; персонал РКТС.

Основной особенностью функционирования системы защиты информации при взаимодействии региональных корпоративных телекоммуникационных сетей с сетью общего пользования является тот факт, что ключевыми функциями по защите информации, которые должна реализовывать система защиты информации (СЗИ) любого предприятия (организации) при взаимодействии РКТС с сетью общего пользования (Интернет), являются: засекречивание; установление личности; доказательство права собственности; предъявление полномочий; проверка подлинности; подтверждение даты действия; удостоверение источника или получателя и т.п., т.е., функции, осуществляемые в электронной форме.

При этом в качестве защищаемых объектов при взаимодействии РКТС с глобальной сетью Интернет должны рассматриваться информация и все ее носители (отдельные компоненты и автоматизированная система обработки информации предприятия (организации) в целом).

Другой особенностью функционирования СЗИ при взаимодействии РКТС с глобальной сетью Интернет, является то, что обеспечение информационной безопасности предполагает создание дополнительных, более сложных препятствий для любого несанкционированного вмешательства в процесс функционирования СЗИ и РКТС, а также препятствий для попыток хищения, модификации, выведения из строя или разрушения их компонентов, то есть, защиту всех компонентов РКТС: оборудования, программного обеспечения, данных (информации) и персонала.

В этом смысле защита информации от несанкционированного доступа (НСД) является только частью общей проблемы обеспечения информационной безопасности при взаимодействии РКТС с глобальной сетью Интернет, а сам термин НСД было бы правильнее трактовать не как «несанкционированный доступ» (к информации), а шире, как «несанкционированные (неправомерные) действия», наносящие ущерб субъектам информационных отношений.

Важность и сложность проблемы защиты информации при взаимодействии РКТС с глобальной сетью Интернет требует принятия кардинальных мер в соответствии с руководящими документами [1, 2], выработки рациональных решений, для чего необходимо сконцентрировать усилия на вопросах разработки общей концепции защиты интересов всех субъектов информационных отношений с учетом особенностей той прикладной области, в которой функционируют различные РКТС.

Более того, концепция защиты информации при взаимодействии РКТС с сетью общего пользования должна предусматривать не только новые технологии защиты, но и адаптивное поведение средств защиты, способное подстраиваться под уровень потенциальных угроз [3]. При этом важную роль играют современные методы анализа (оценивания) защищенности, методы оценивания эффективности функционирования СЗИ [4, 5].

Заключение. Именно поэтому СЗИ, предназначенная для реализации политики безопасности при взаимодействии РКТС с глобальной сетью Интернет, на наш взгляд, в самом общем виде может быть определена как организованная совокупность всех современных средств, методов и мероприятий, выделяемых (предусматриваемых) в РКТС для решения в них выбранных задач защиты. Задачи же защиты информации при взаимодействии РКТС с глобальной сетью Интернет решаются с целью нейтрализации дестабилизирующего воздействия причин нарушения целостности информации при обеспечении физической целостности информации или с целью перекрытия каналов несанкционированного получения информации – при защите от несанкционированного получения информации.

Таким образом, современная система защиты, предназначенная для обеспечения доступности, конфиденциальности и целостности информации, хранимой и передаваемой при взаимодействии РКТС с сетью общего пользования, представляет собой не просто взаимоувязанную по месту, времени и задачам совокупность средств, методов защиты информации и персонала.

Это целый комплекс гибких, адекватных потенциальным угрозам организационных и технических мер, направленных на обеспечение информационной безопасности предприятия (организации). Причем, говоря о «комплексе» мер, необходимо иметь в виду использование при взаимодействии РКТС с сетью общего пользования, не только технических средств защиты, но также мер административного и правового характера.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 53109-2008. Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности.
2. ГОСТ Р 52448-2005. Обеспечение безопасности сетей электросвязи.
3. Авраменко В.С. Адаптивный контроль защищенности информации от несанкционированного доступа на основе информационных образов. // Проблемы информационной безопасности. Компьютерные системы. 2010. № 2. С. 45-49.
4. Авраменко В.С. Оценка защищенности информации на основе теории нечетких множеств. // Вопросы радиоэлектроники. 2014. Т. 3. № 1. С. 142-148.
5. Паращук И.Б., Аверьянов Е.Г. Формулировка целей, задач и принципов адаптивного мониторинга информационной безопасности телекоммуникационных сетей. // Актуальные проблемы защиты и безопасности: Труды XVII Всероссийской научно-практической конференции РАРАН. Том 5. – СПб.: ФГБУ «РАРАН», 2014. – 208 с. С. 26-31.

УДК621.391(075.8)

ТИПЫ СРЕДСТВ ДОВЕРЕННОЙ ЗАГРУЗКИ И ИХ РОЛЬ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Жмуров Владислав Дмитриевич[1], Паращук Игорь Борисович[2], Саяркин Леонид Андреевич[1]
[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mails: shchuk@rambler.ru, sayarkin95@mail.ru

Аннотация. Рассмотрены типы современных средств доверенной загрузки и особенности подходов к формулировке понятия «доверенная загрузка». Проанализирована роль различных средств доверенной загрузки в структуре системы защиты и функции, реализуемые ими для разных уровней архитектуры компьютера в составе автоматизированного рабочего места администратора или пользователя телекоммуникационной сети.

Ключевые слова: *доверенная загрузка; автоматизированное рабочее место; уровень; защита; доступ; функции.*

TYPES OF MEANS OF TRUSTED DOWNLOADS FACILITIES AND THEIR ROLE IN SECURING THE INFORMATION SECURITY OF TELECOMMUNICATION NETWORKS

Zhmurov Vladislav[1], Parashchuk Igor[2], Sayarkin Leonid[1]
[1]Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
[2] St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
e-mails: shchuk@rambler.ru, sayarkin95@mail.ru

Abstract. Types of modern means of trusted loading and features of approaches to the formulation of the concept of "trusted download" are considered. The role of various means of trusted loading in the structure of the protection system and the functions implemented by them for different levels of the computer architecture in the automated workplace of the administrator or the user of the telecommunications network is analyzed.

Keywords: *trusted download; the automated workplace; level; protection; access; functions.*

Известно, что развитие и совершенствование средств защиты идет по трем основным направлениям: 1-ое направление: разрабатываются и модифицируются средства в составе операционной системы (ОС) – средства идентификации и аутентификации; средства разграничения доступа; средства оперативного наблюдения; средства аудита; средства контроля целостности информации, циркулирующей в телекоммуникационных сетях (ТКС) и системы защиты информации (СЗИ); средства работы с внешними носителями; средства маркировки документов; средства тестирования элементов СЗИ ТКС; 2-ое направление: разрабатываются и модифицируются средства в составе общего программного обеспечения (ПО) и функционального ПО – средства дополнительной аутентификации; средства разграничения доступа; средства взаимодействия с ядром СЗИ ТКС и средства маркировки документов; 3-е направление: совершенствуются внешние средства защиты от несанкционированного доступа (НСД), к которым относят внешние компоненты средств контроля целостности ТКС и СЗИ; внешние компоненты средств контроля работоспособности СЗИ; компоненты защиты доступа к внутренним элементам технических средств; средства работы с внешними носителями, а также аппаратно-программные средства доверенной загрузки.

Рассмотрим несколько распространенных подходов к формулировке понятия «доверенная загрузка». Например, доверенная загрузка – регламентированное Руководящими документами применение программных и программно-технических средств, используемых в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом и реализующих функции по предотвращению несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники на этапе его загрузки (далее – средства доверенной загрузки) [1].

Зачастую под доверенной загрузкой понимается загрузка ОС с внутреннего жесткого диска компьютера, которая происходит только после выполнения процедур идентификации и аутентификации пользователя, а также проверки целостности программной и аппаратной среды рабочего места, в том числе целостности объектов загружаемой ОС. При этом должна обеспечиваться невозможность загрузки пользователем другой ОС (с внешних носителей информации и др.) [2]. Нередко под доверенной загрузкой принято считать загрузку различных ОС только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств персонального компьютера (ПК) или другого терминала на автоматизированном рабочем месте (АРМ) пользователя ТКС – с использованием механизма пошагового контроля целостности, а также аппаратной идентификации и аутентификации этого пользователя [3]. Другими словами, в этом режиме загрузка различных ОС ПК либо иного терминала ТКС осуществляется только в том случае, если подтверждено, что в ПК не произошло никаких несанкционированных изменений (на аппаратном уровне и в критичной части приложений) и что включает его именно тот пользователь ТКС, который имеет право на нем работать именно в это время [4].

Процесс доверенной загрузки ПК в составе АРМ пользователя ТКС необходим для того, чтобы воспрепятствовать несанкционированному запуску ПК пользователя, загрузке операционной системы

и получению возможности доступа к конфиденциальной информации. Причем в сферу действия средств доверенной загрузки входят этапы работы компьютера или другого терминала на АРМ пользователя ТКС от запуска микропрограммы базовой системы ввода-вывода (BIOS) до начала загрузки операционной системы [3]. При этом доверенная загрузка включает в себя аутентификацию пользователя; контроль устройства (жесткого диска или другого носителя), с которого BIOS начинает загрузку ОС; контроль целостности и достоверности загрузочного сектора устройства и системных файлов запускаемой ОС; шифрование и дешифрование загрузочного сектора, системных файлов ОС, либо шифрование всех данных устройства, а также аутентификацию, шифрование и хранение режимных (конфиденциальных) данных, таких как ключи и контрольные суммы [3].

Известны три основных типа средств доверенной загрузки [1, 4]: средства доверенной загрузки уровня базовой системы ввода-вывода; средства доверенной загрузки уровня платы расширения (программно-аппаратные средства доверенной загрузки); средства доверенной загрузки уровня загрузочной записи. Причем для дифференциации требований к функциям безопасности средств доверенной загрузки выделяются шесть классов защиты средств доверенной загрузки. Самый низкий класс – шестой, самый высокий – первый [1].

Средства доверенной загрузки уровня базовой системы ввода-вывода обычно тесно интегрированы с прошивкой материнской платы, активируются прямым вызовом из базовой системы ввода-вывода, пользуются всеми защитными функциями контроллера доступа к внутренней памяти, не требуют дополнительных затрат на установку и эксплуатацию, при покупке обходятся дешевле по сравнению с программно-аппаратными устанавливаемыми решениями [4, 5].

Программно-аппаратные средства доверенной загрузки обычно устанавливаются на плату (шину) расширения и позволяют, при подаче питания на устройство и получении управления, выполнять контроль целостности конфигурации и логических объектов на накопителях данных [1, 4].

Средства доверенной загрузки уровня загрузочной записи являются решением, обеспечивающим (в большей степени) недоступность пользовательских данных с помощью нестандартного форматирования и (или) шифрования носителя этих данных. Этими средствами не обеспечивается защита от загрузки нештатных операционных систем и несанкционированного использования компьютерного оборудования [4].

Заключение. Таким образом, существующие типы средств доверенной загрузки предназначены каждый для конкретных целей и для конкретных уровней защищаемых элементов АРМ пользователей ТКС, их применение должно осуществляться комплексно, с учетом уровня существующих угроз. Вместе с тем, роль комплексов, модулей и иных средств доверенной загрузки в обеспечении информационной безопасности телекоммуникационных сетей достаточно велика и потенциал их применения объективно возрастает, это одни из немногих систем, позволяющих без больших финансовых затрат, оперативно и гарантированно предотвращать несанкционированный доступ к программным и техническим ресурсам средств сбора, обработки, хранения и передачи информации в ТКС на этапе их загрузки.

СПИСОК ЛИТЕРАТУРЫ

1. Требования к средствам доверенной загрузки. // Информационное письмо ФСТЭК России от 06.02.2014 №240/24/405 «Об утверждении Требований к сдедствам доверенной загрузки» в соответствии с Приказом ФСТЭК России от 27.09.2013 № 119). [Электронный ресурс]: http://fstec.ru/normotvorcheskaya/793.
2. Никитин Е.А., Шрамко В.А. Всегда ли на замке? Как обезопасить компьютер модулем доверенной загрузки. // Vikotenik. №20 (Август), 2010. // [Электронный ресурс]: http://vikotenik.livejournal.com/226909.html.
3. Конявский В.А. Управление защитой информации на базе СЗИ НСД «Аккорд». – М.: Радио и связь, 1999. – 325 с.
4. Левенков О.А. Средства доверенной загрузки. // Технологии безопасности. №6, 2013 С. 40-41.
5. Авраменко В.С., Домбровский Я.А., Бобрешов-Шишов Д.И. и др. Совершенствование средств обеспечения доверенного сеанса работы при эксплуатации автоматизированных систем управления. // Естественные и технические науки. 2016. № 11 (101). С. 207-214.

УДК 004.725.5 + 004.056.5

СПОСОБ ЗАЩИТЫ РЕСУРСОВ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ

Журавель Евгений Павлович
Санкт-Петербургский политехнический университет Петра Великого
Россия, Санкт-Петербург, ул. Политехническая, 29
e-mail: eshur2003@mail.ru

Аннотация. В статье сформулирован подход к защите ресурсов мультисервисной сети связи на основе комплексного анализа априорной и апостериорной информации состояния о ресурсах мультисервисной сети связи. Формирование адекватных мер защиты мультисервисной сети связи предлагается на уровнях её ресурсов и технологий и (или) сред передачи деструктивных воздействий.

Ключевые слова: *мультисервисная сеть связи; сеть управления; сеть обеспечения функционирования; сеть сбора и анализа информации состояния.*

THE WAY OF PROTECTION OF RESOURCES OF A MULTISERVICE COMMUNICATION NETWORK

Zhuravel Evgeny
Peter the Great St. Petersburg Polytechnic University
Russia, St. Petersburg, Politehnicheskaya str., 29
e-mail: eshur2003@mail.ru

Abstract. In article approach to resource protection of a multiservice communication network on the basis of the complex analysis of prior and posteriori information of a status on resources of a multiservice communication network is formulated. Formation of adequate measures of protection of a multiservice communication network is offered at the levels of its resources and technologies and (or) transmission mediums of destructive influences.

Keywords: *multiservice communication network; control plane; operation provisioning plane; collecting and analysis of information state network.*

Введение. Основными характеристиками единой сети электрической связи (ЕСЭС) Российской Федерации (РФ) являются целостность, устойчивость и безопасность её функционирования (п. 1 ст. 41 [1]), соответственно, указанными характеристиками должны обладать и сети ЕСЭС, её составляющие. Модели источников угроз (нарушителей), угроз, деструктивных воздействий, технологий и (или) сред передачи деструктивных воздействий, а также модели ресурсов мультисервисой сети связи (МССС) как основного вида телекоммуникационной сети связи ЕСЭС РФ целесообразно рассмотреть в соответствии с [2] и, на основе результатов рассмотрения, в общем виде сформулировать подход к защите ресурсов МССС, заключающийся в комплексном анализе априорной и апостериорной информации состояния о ресурсах МССС и последующем формировании на его основе адекватных мер защиты МССС на уровнях её ресурсов и технологий и (или) сред передачи деструктивных воздействий.

К вопросам защиты ресурсов МССС следует подходить комплексно, учитывая особенности и взаимосвязи каждой из рассматриваемых моделей обобщённой модели воздействий на ресурсы МССС, общие теоретические и практические результаты по построению систем защиты и требования руководящих документов, федеральных законов (ФЗ) РФ отрасли связи и смежных отраслей. В соответствии с п. 7 ст. 24, п. 1 ст. 25, пп. 10 - 11 ст. 24, ФЗ [1] и п. 6 ст. 3, п. 2 ст. 4, пп. 1-2 ст. 6 ФЗ [3] обеспечение безопасности МССС целесообразно рассматривать на основе национальных стандартов (НС) РФ, которое, в соответствии с НС [4], представляет собой совокупность:

– организационных (правовых) мероприятий по защите ресурсов МССС (федеральные законы, инструкции, руководящие документы, ведомственные и национальные стандарты, специальные требования и рекомендации, подзаконные акты (регламенты, письма) и др.);

– технических (физических) мероприятий по защите (ограничение физического доступа к защищаемым ресурсам, технически и научно обоснованное формирование контролируемой зоны и др.);

– технических средств защиты от утечки за счет побочных электромагнитных излучений и наводок (технические средства генерации шумов, технические средства физической (гальванической) развязки электропитания и др.);

– программных средств защиты (антивирусы, средства контроля целостности, криптографические средства, программные межсетевые экраны, тематические исследования микропрограммного, общего, специального и др. обеспечений функционирования телекоммуникационного оборудования (ТКО) и средств вычислительной техники (СВТ) и др.);

– программно-технических средств защиты (аппаратно-программные модули доверенной загрузки, аппаратно-программные криптографические средства, аппаратно-программные межсетевые экраны, шлюзы однонаправленной передачи данных и др.).

Каждое из перечисленных выше мероприятий и средств механизма обеспечения безопасности системы на соответствующих этапах ее жизненного цикла в соответствии с [5,6] и НС [7,8] может и должно включать в себя следующие виды требований безопасности:

– активные;
– пассивные;
– проактивные.

Активные требования безопасности рассматриваются в НС [7], соответствуют активному аспекту защиты и включают в себя функциональные требования, предъявляемые к функциям безопасности системы и реализующим их механизмам.

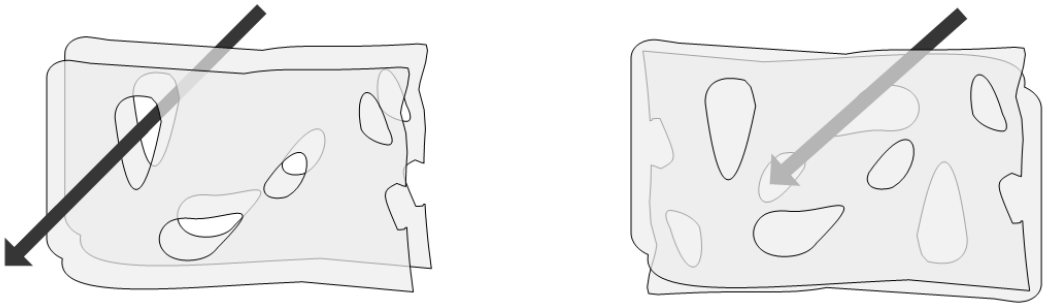
Пассивные требования безопасности рассматриваются в НС [8], соответствуют пассивному аспекту защиты и включают в себя требования доверия, предъявляемые к технологиям и процессам разработки системы, а также к процессам ее эксплуатации и развития.

Применительно к этапам жизненного цикла услуг [9, 10] и ресурсов [11, 12] МССС целесообразно выделить в отдельный вид проактивные требования безопасности, являющиеся одним из перспективных и развивающихся направлений совершенствования механизмов

обеспечения безопасности, представляющие собой совокупность взаимодополняющих активных и пассивных требований безопасности, формулируемых с использованием, в том числе, методов интеллектуального анализа данных и реализуемых, в том числе, на основе аналитических информационных систем [5, 6].

Модель защиты мультисервисной сети связи.

Для построения модели защиты МССС целесообразно использование разработанной в 1990 г. Д. Ризоном из Манчестерского университета Великобритании модели определения и описания ситуаций, потенциально ведущих к наступлению некоторого не приемлемого события, которая получила название модели "швейцарского сыра" [13]. В этой модели, схематично показанной на рисунке 1 а, траектория от начального события ("предпосылки"), до конечного не приемлемого события ("инцидента", "происшествия", "катастрофы") последовательно проходит через условные отверстия ("ошибки", "риски", "дырки") соответствующей им пространственной области каждого уровня ("пластины сыра", "ломтика сыра"). Если в очередном уровне в той же пространственной области отверстия нет, то событие не произойдет (рисунок 1б).



а) б)

Рис. 1. Модель "швейцарского сыра"

Таким образом, наступление некоторого не приемлемого события является результатом сочетания возможностей для его наступления на каждом уровне. Применительно к обобщённой модели воздействий на ресурсы МССС это означает, что должен быть источник угроз (нарушитель), который должен формировать угрозу, которая должна оказывать воздействие, способное быть переданным с использованием среды передачи и, в той или иной мере, соответствовать ресурсам МССС. При этом если какую-либо взаимосвязь обобщённой модели воздействий на ресурсы МССС удастся разорвать, то воздействия не произойдет.

Модель "швейцарского сыра" получила широкое применение в авиации, здравоохранении и, с некоторыми изменениями и дополнениями, может быть использована для защиты объектов информационной безопасности информационно-телекоммуникационных систем, например, так, как это предложено в [14]. Вместе с тем, при формировании способа защиты ресурсов МССС следует учитывать не только вопросы обеспечения информационной безопасности, но и вопросы обеспечения устойчивости и безопасности МССС в совокупности, в том числе, вопросы технической безопасности (катастрофоустойчивое расположение точек присутствия ТКО, контроль доступа к ресурсам и др.), вопросы технологической безопасности (технологическая независимость от зарубежных производителей ТКО и др.), вопросы безопасности технологий и средств передачи информации (протоколы, их применение и др.), вопросы безопасности общего (офисного и др.) и специального программного обеспечения и др. Функциональные возможности элементов ресурсов МССС, возможные варианты и особенности их построения и функционирования как элементов сложной системы, обладающей интегративными свойствами, следует использовать с максимально полным выполнением формулируемых выше активных, пассивных и проактивных требований безопасности.

В [15] рассмотрен один из вариантов реализации защиты МССС на уровнях её ресурсов и технологий и (или) сред передачи, под которым понимается статическое выделение в МССС сети обеспечения функционирования и сети, непосредственно реализующей контур управления.

Сеть управления предлагается использовать как основу для кроссплатформенной системы управления оборудованием МССС на основе принципов автоматизированного конфигурирования сетевых устройств с использованием протоколов безопасного сетевого соединения, таких как протоколы Simple Object Access Protocol (SOAP), CPE WAN management protocol (CWMP), eXtensible Markup Language (XML), XML Network Management Protocol (XMLNMP) инкапсулированные в протокол HyperText Transfer Protocol Secure, (HTTPS), протокол Transaction Language 1 (TL1), протокол Simple Network Management Protocol (SNMP) версии 3 с расширением SNMP trap, протокол Secure Shell (SSH) версии 2 и др. Также сеть управления может использоваться для резервного копирования конфигураций сетевого оборудования с использованием протокола SSH File Transfer Protocol (SFTP), метода put протокола File Transfer Protocol (FTP) в реализации vsftpd, протокола Secure Copy (scp)

использующего SSH, методы put и post протокола HTTPS и др., что позволит автоматизировать отслеживание изменений в конфигурации сетевых устройств, например, с использованием систем контроля версий Concurrent Versions System (CVS), Subversion, Git, Web Distributed Authoring and Versioning (WebDAV) и др.

Сеть обеспечения функционирования реализует функции обеспечения синхронизации точного времени с использованием протокола Network Time Protocol (NTP), которое используется в МССС с коммутацией пакетов вместо систем тактовой синхронизации синхронных сетей, функции именования сетевых элементов на основе единого указателя ресурсов Uniform Resource Locator (URL) с использованием системы доменных имён Domain Name System (DNS), функции сетевой идентификации с использованием опций 43, 60 и 82 протокола Dynamic Host Configuration Protocol (DHCP) версии 4, опций 16, 17 и 18 протокола DHCP версии 6 и (или) функции аутентификации, авторизации и учёта использования услуг с использованием протокола Remote Authentication in Dial-In User Service (RADIUS), протокола Terminal Access Controller Access Control System plus (TACACS+), протокола DIAMETER, протокола Lightweight Directory Access Protocol (LDAP), протокола System for Cross-Domain Identity Management (SCIM) и др. При этом, функция сетевой идентификации и указанные выше протоколы могут быть объединены в иерархию с целью формирования услуги "Удостоверение как услуга" для пользователя и (или) программного обеспечения ТКО и (или) СВТ.

Построение предлагаемых технологических сетей управления и обеспечения функционирования для экономии ресурсов целесообразно выполнить программно с использованием технического ресурса сети общего пользования средствами виртуализации ТКО и общего программного обеспечения ЭВМ, то есть отделения одного вида трафика от другого с использованием реализаций, позволяющих тем или иным способом виртуализировать физический порт и (или) логический сетевой ip/ppp-интерфейс. Одним из таких достаточно широко используемых средств виртуализации является использование стандарта 802.1q, позволяющего выделять виртуальные сети (Virtual Local Area Network, VLAN) на уровне звена данных эталонной модели взаимодействия открытых систем (ЭМВОС) МССС данного оператора связи, в том числе, с поддержкой пропуска трафика таким же (или другим) способом выделенных сетей МССС другого оператора связи.

Способ защиты ресурсов мультисервисной сети связи.

Приняв предложенные в [13] и [15] модель и подход реализации защиты МССС за основу, рассмотрим следующий способ защиты ресурсов МССС на уровнях ресурсов и технологий и (или) сред передачи деструктивных воздействий дополнением, взаимным построением и определением функционального назначения составляющих ее ресурсов в соответствии с формулируемыми требованиями. Особенностью технических, программных и программно-технических воздействий на ресурсы МССС является то, что они могут быть оказаны на ресурсы любой из составляющих ее сетей (см. рисунок 2), причем не только последовательно, как в модели защиты [13], но и параллельно и (или) последовательно-параллельно. Данная особенность обусловлена тем, что, например, нормальная (средняя) нагрузка передачи данных в каждой из соответствующих сетей доступа может, в совокупности, стать критической как уже в сетях агрегации, так и, например, на пограничном оборудовании, относящимся к транспортной сети МССС. Другим примером может являться вновь выявленная уязвимость в микропрограммном обеспечении зарубежного (не доверенного) ТКО сети агрегации МССС, позволяющая осуществлять удаленные деструктивные воздействия или оказывающая влияние на процессы функционирования данного ТКО.

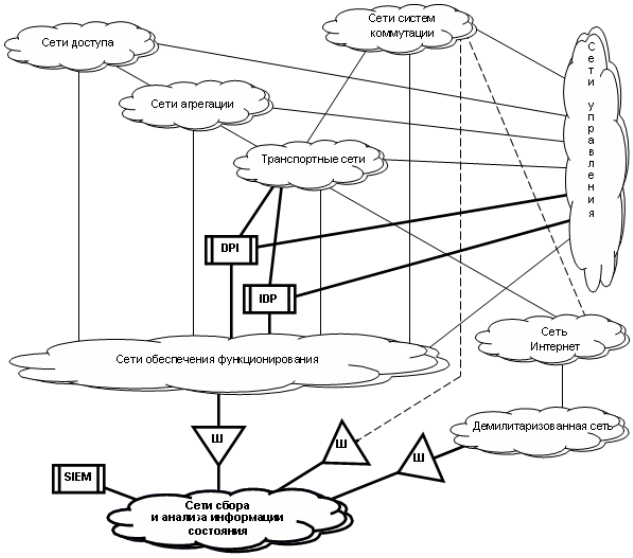


Рис. 2. Структура защищенной мультисервисной сети связи (вариант)

К введенным в [15] сетям управления и сетям обеспечения функционирования в соответствии с выполняемыми ими функциями подсоединены сети доступа, сети агрегации, транспортные сети и сети систем коммутации соответственно (последние – в случае, если эти сети принадлежат данной организации связи). Присоединение по управлению подразумевает двусторонний обмен информацией [16] и, как следствие, в случае реализации проникновения в соответствующие ресурсы МССС, потенциальную возможность для нарушителя (источника угроз) осуществить подчистку (стирание, изменение, маскирование и др.) соответствующей информации о его действиях или другой информации. В связи с этим, целесообразно физически выделить отдельную сеть для сбора и анализа информации состояния ресурсов МССС и однонаправлено присоединить к ней сеть обеспечения функционирования с использованием, например, имеющихся программно-аппаратных решений шлюза односторонней передачи данных (ШОПД) [17], которые обозначены на рисунке 2 буквой "Ш" и позволяют осуществлять однонаправленную передачу информации на основе протоколов syslog, syslog-tls, User Datagram Protocol (UDP) или других протоколов прикладного уровня ЭМВОС.

В МССС выделяют ТКО и СВТ, составляющие так называемую демилитаризованную сеть, не имеющую подключения к сетям управления и обеспечения функционирования данной МССС, управление ресурсами которой осуществляется с использованием специальных средств и способов управления (непосредственные команды с локальной физической консоли, сеансовые ключи, одноразовые пароли, виртуальная частная сеть, специальные решения для существующих протоколов управления и др.). ТКО и СВТ демилитаризованной сети осуществляет функционирование по предназначению как для пользователей сетей, составляющих данную МССС, так для пользователей сети Интернет. К составляющим их ресурсам относятся СВТ, обеспечивающие функционирование внешних службы доменных имен (Domain Name Service, DNS), службы обмена сообщениями электронной почты (mail exchange), службы World Wide Web, службы антивирусного контроля и др., а также ТКО, осуществляющее сетевое присоединение СВТ, межсетевое экранирование, роутинг, трансляцию адресов и др. Для контроля ресурсов, составляющих демилитаризованную сеть, ее также целесообразно однонаправлено присоединить к сети сбора и анализа информации через ШОПД и, по возможности, использовать для передачи данных протоколы syslog-tls и UDP. К сети сбора и анализа информации через ШОПД следует, по возможности, подключать и сети систем коммутации, которые имеют иного собственника и осуществляют предоставление услуг в рассматриваемой МССС.

Оценка качества способа защиты ресурсов мультисервисной сети связи.

Недостатками физического выделения сети для сбора и анализа информации и использования протокола UDP являются некоторые затраты ресурсов, необходимые для формирования физически выделенной сети и не подтверждаемый (не гарантированный) прием информации. Уменьшение затрат ресурсов сокращением количества ШОПД, например, до двух (см. рисунок 3) и использованием роутера, не обеспечивает требуемого уровня защиты в связи с тем, что роутер не находится под мониторингом и управлением сетей управления и обеспечения функционирования.

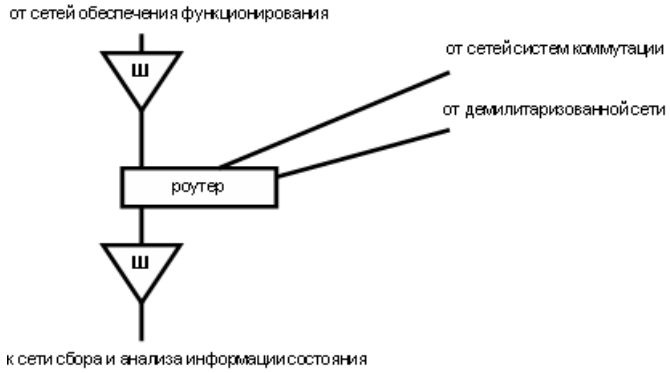


Рис. 3. Вариант подключения шлюзов однонаправленной передачи данных.

Это, в свою очередь, может привести к тому, что очередное обновление микропрограммного обеспечения данного роутера, которое в достаточно крупных организациях связи осуществляется централизованно по плану для всего оборудования данного вида, в соответствии с регламентами, дизайном сети и с использованием шаблонов, в результате может образовать какой-либо "шаблонный" интерфейс на сетевом уровне ЭМВОС и позволить нарушителю (источнику угроз) получить удаленное управление данным маршрутизатором с последующим перехватом системных сообщений, выявлением действительных наименований учетных записей (логинов) пользователей, версий технического обеспечения ТКО и СВТ, версий общего и специального программного обеспечения ТКО и СВТ и др. Установка межсетевого экрана между роутером и подключаемыми к нему внешними сетями отчасти может ослабить данные угрозы, однако результирующее решение не

будет отвечать требованию минимизации затрат ресурсов, а не подключенный к сетям управления и обеспечения функционирования межсетевой экран может быть подвержен перечисленным выше и другим рискам.

Достоинством предлагаемого способа защиты МССС является не возможность изменения информации нарушителем (источником угроз), который, получив доступ к некоторым ресурсам МССС, может остановить функционирование процесса передачи информации состояния. Для ослабления данного недостатка следует реализовать мониторинг периодичности поступающей информации от ресурсов МССС, состоящий из следующих действий:

– выявление и сохранение первого сообщения syslog (syslog-tls) от данного хоста, характеризующегося датой, mac-адресом, доменным именем (hostname), IPv4-адресом и (или) IPv6-адресом (в зависимости от настроек syslogd) и наличием либо отсутствием использования TLS (портом назначения сообщения);

– осуществление контроля поступления сообщений от каждого из сохраненных хостов в течение, например, каждого часа и, при не поступлении ни одного сообщения и (или) при изменении значений параметров (характеристик сообщений, срабатывания правил динамически подключаемых модулей аутентификации и др.), формирование и выдача соответствующих сообщений и (или) предупреждений администратору безопасности;

– маскирование сообщений и (или) предупреждений администратору безопасности об отсутствии поступления сообщений от каждого из сохраненных хостов с реализацией безусловного маскирования и маскирования на некоторое время до выполнения плановых (регламентных) работ.

В сети сбора и анализа информации целесообразно выполнение периодического и/или ретроспективного автоматизированного анализа собранной информации с использованием соответствующих методов представления и использования знаний, методов искусственного интеллекта, методов нечёткой логики или других методов и подходов [5, 6]. Так, например, в системах управления событиями и информационной безопасностью (Security Information and Event Management, SIEM), реализованы алгоритмы корреляции системных сообщений, поступающих от ресурсов МССС, позволяющие выявлять сложные распределённые сценарии атак на ресурсы МССС, состоящие из множества распределенных во времени действий, каждое из которых по отдельности не расценивается как потенциально опасное, также позволяющие формировать и выдавать соответствующие сообщения и (или) предупреждения администратору безопасности [18].

Еще одним недостатком предлагаемого технического решения по физическому выделению сети сбора и анализа информации является то, что оно позволяет выявлять сложные распределенные воздействия, например, с использованием SIEM-систем, но от момента воздействия до его выявления может пройти некоторое существенное для предоставления услуг и управления ресурсами МССС время. В общем случае значения параметров (характеристик) воздействий на услуги и ресурсы МССС не известны и не могут быть получены априорно. В связи с этим, помимо формулируемого выделения сети сбора и анализа информации для защиты МССС на уровне ресурсов, протоколов и (или) сред передачи целесообразно использование динамических алгоритмов, например, таких, как рассмотренный в [19], которые позволяют выполнять поиск деструктивных воздействий и их оперативную идентификацию в режиме, близком к "жёсткому" реальному времени за счёт реализации параллельной структурной идентификации пакетов широкого спектра протоколов пакетной передачи данных, а также обнаружения последовательностей повторяющихся пакетов с контролем допустимых интервалов их следования при наличии априорно достоверной информации об используемых протоколах. В совокупности, это позволяет выполнять идентификацию протоколов путём структурного анализа пакетов и осуществлять динамическую защиту ресурсов МССС от возможных деструктивных воздействий. Дальнейшим развитием динамических алгоритмов могут являться варианты управляющих воздействий для поддержания в работоспособном состоянии (сценарии защиты) ресурсов МССС, такие как изменение значимых бит в процессе работы устройства поиска информации и (или) блокирование определённых портов и (или) одного или нескольких ресурсов (ip-адресов) МССС и (или) корректировка настроек межсетевых экранов и (или) сетевых маршрутов одного или нескольких ресурсов МССС и др.) в соответствии с накопленными по состоянию на соответствующий момент времени функционирования МССС статистическими оценками результатов деструктивных воздействий, т.е. активное противодействие выявляемым деструктивным воздействиям. Вместе с тем, ввиду возможных ложных срабатываний при реализации активных мер защиты разработка активных требований безопасности и реализующих их активных мер защиты требует проведения дальнейших исследований.

В настоящее время средства реализации динамических алгоритмов поиска деструктивных воздействий принято разделять на [20, 21]:

– средства выполнения статистического анализа, накопления статистических данных, фильтрации пакетов в соответствии с их содержимым на уровнях начиная с уровня звена данных и до прикладного уровня ЭМВОС включительно, а также управлением качеством предоставляемых МССС услуг регулированием полосы пропускания отдельных приложений на соответствующем уровне ЭМВОС (Deep Packet Inspection, DPI) [20];

– средства выявления и предотвращения воздействий, выполняющие углубленный поиск аномальной сетевой активности, формируемой в большинстве случаев, на прикладном уровне ЭМВОС компьютерными вирусами и сетевыми "червями" и предотвращающие (блокирующие) выявленный источник (ip-адрес и (или) сокет ip-адреса) такой активности (Intrusion Detection and Prevention, IDP) [21].

В МССС целесообразно использование DPI и IDP в совокупности. Подключение DPI и IDP следует осуществить к ресурсам транспортных сетей без изменения существующей топологии МССС (см. рисунок 2) и, для применения по предназначению, выполнять на эти устройства зеркалирование трафика соответствующих сетей стандартными средствами ТКО МССС на уровне звена данных с использованием VLAN и, возможно, с указанием соответствующих подсетей IP-адресов, динамически путем периодического, (например, каждые 4 часа) переопределения значений источников зеркалируемого трафика и (или) статически (например, на одну – две недели) в случае выявления аномалий в значениях анализируемого трафика соответствующей подсети МССС.

Для настройки и проверки корректности функционирования и срабатывания правил DPI, IDP и SIEM систем в части выявления нагрузочных аномалий трафика ТКО и (или) аномальной нагрузки служб СВТ МССС целесообразно использовать программные средства нагрузочного тестирования служб МССС, такие как iPerf, DHCPerf, DNSPerf, HTTPerf, NetPerfff и др., с реализованными в них расчетами значений метрик производительности соответствующих служб и последующим выявлением и настройкой порогов срабатывания правил в DPI и IDP. При необходимости выполнения более глубокой оценки защищенности МССС от деструктивных воздействий на уровне протоколов и (или) сред передачи деструктивных воздействий целесообразно использовать программные средства генерации требуемых видов трафика, таких как OSTINATO, Seagull и др., с выполнением "тонких" настроек соответствующих сценариев воздействий на ресурсы МССС.

Предлагаемый способ защиты МССС за счет введенной новой совокупности существенных признаков взаимодействия ресурсов МССС (выделенных более толстыми линиями на рисунке 2), позволяет осуществлять выявление и предотвращение воздействий на ресурсы МССС и предоставляемые ею услуги на уровне ее ресурсов, протоколов и (или) сред передачи деструктивных воздействий. Так, например, любое изменение в конфигурации ТКО и СВТ МССС будет выявлено с использованием соответствующих функций программного обеспечения сети управления МССС, аномалии (атаки) в трафике пользователей (его характеристики в части спама, сетевой вирусной активности и др.), будут выявлены средствами IDP, аномалии (атаки) в трафике Интернет (характеристики кадров, пакетов, блоков и, частично, данных) будут выявлены средствами DPI, аномалии (атаки) на СВТ МССС в сетях систем коммутации и демилитаризованной сети (отказ в обслуживании, попытки перехвата управления, фиксации попыток вторжения и их результатов и др.) будут выявлены с использованием SIEM-систем сети сбора и анализа информации состояния МССС, а также, для мониторируемых и управляемых ресурсов соответствующих сетей, могут быть выявлены по косвенным признакам значений параметров, собираемым в сети управления МССС (повышение температуры процессоров, увеличение количества принятой и переданной информации на порту, увеличение объема используемой оперативной памяти, увеличение объема используемой swap-памяти, попытки открытия сессии не из диапазонов IP-адресов сети управления, переход в привилегированный режим, выполнение команд привилегированного режима и др.).

Следует отдельно отметить, что системный администратор (общего программного обеспечения и специального программного обеспечения), сетевой администратор, администратор баз данных и администратор безопасности, обеспечивающие функционирование МССС по предназначению, не рассматриваются как нарушители (источники угроз) безопасности МССС, поскольку принимается, что их соответствие исполняемым функциям достигается иными, например, организационными методами. В связи с этим, для повышения качества предлагаемых технических решений по защите МССС на уровнях ее ресурсов и технологий и (или) сред передачи, необходимо уточнить регламент работы данных технических специалистов, непосредственно обеспечивающих функционирование МССС по предназначению, выполняющих и (или) контролирующих выполнение требований безопасности. Каждый специалист в зоне своей ответственности должен осуществлять периодический мониторинг информации состояния управляемых и, соответственно, мониторируемых им ТКО и СВТ МССС, не только принимая к сведению отчеты соответствующих автоматизированных систем и, на их основе, формируя (корректируя) меры защиты, но и периодически непосредственно просматривая "сырую" статистическую информацию состояния "критических" систем аутентификации, авторизации и аккаунтинга (radacct, syslog и др.) в графическом пользовательском интерфейсе и (или) непосредственно в интерфейсе командной строки с целью соотнесения её с имеющимися открытыми (опубликованные и известные уязвимости) и ограниченного пользования сведениями о вновь выявляемых уязвимостях в ТКО и СВТ МССС (уязвимости, для которых еще не выпущены обновления, но анонсирован их выпуск, не известные уязвимости "нулевого" дня и пр.), не ожидая выпуска централизованных обновлений для соответствующих автоматизированных систем. Также целесообразно осуществление частичной функциональной взаимозаменяемости, т.е. периодическое выполнение соответствующего вида работ данным специалистом вместо какого-либо другого

специалиста, что может быть оправдано как с позиции одного из вариантов частичного организационного решения вопросов доверия ("кто будет сторожить сторожей?"), так и с позиции решения вопросов взаимозаменяемости на период отпуска, болезни и (или) иных изменений в штатном расписании.

В целом, предлагаемый способ защиты ресурсов МССС позволяет расширить набор типовых сетевых сценариев, приведенных в НС [22] и не противоречит п. 2 ст. 15 ФЗ [1]. В результате, при некоторых начальных затратах на проектирование, построение и разработку шаблонов конфигурации для используемых ресурсов МССС, в дальнейшем упрощается построение систем мониторинга и управления, уменьшается стоимость технической эксплуатации и существенно снижаются риски воздействий на ресурсы МССС.

Заключение.Рассмотренный способ защиты ресурсов МССС может применяться на этапах планирования, построения и эксплуатации МССС и, наряду с комплексным применением других средств (например, антивирусных средств, средств контроля изменений, средств построения виртуальных частных сетей, реализаций TLS/SSL и др.), позволяет осуществить формирование защищенной структуры ресурсов МССС что, в совокупности, существенно снижает риски воздействий на ресурсы МССС, но, к сожалению, не устраняет их полностью. Не смотря на явные и потенциальные технические, программные, активные, пассивные и проактивные возможности по выявлению, снижению и (или) ослаблению деструктивных воздействий с использованием формулируемого выше способа защиты МССС следует отметить, что угрозы безопасности МССС будут существовать до тех пор, пока существуют ресурсы МССС, требующие защиты, существуют пользователи и администраторы услуг и (или) ресурсов МССС, подчас являющиеся нарушителями (источниками угроз) безопасности или создающие предпосылки к нарушениям безопасности, существуют и развиваются МССС, используемые ими технологии и протоколы, а также существует окружающая среда, в которой находятся пользователи, администраторы и функционирует МССС. Таким образом, представляется целесообразным как дальнейшее периодическое уточнение существующих, так и разработка новых моделей, методик, профилей, способов, систем и средств для формирования адекватных (достаточных) мер защиты МССС на уровнях её ресурсов и технологий и (или) сред передачи деструктивных воздействий, актуализация и применение которых в совокупности позволит достигать требуемого уровня функциональной, технической и технологической безопасности МССС.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон Российской Федерации от 7 июля 2003 г. №126-ФЗ "О связи" (в ред. 06.07.2016 г.). Доступ из справ.-правовой системы полнотекстовой базы данных.
2. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. М. : Стандартинформ, 2014. 51 с.
3. Федеральный закон Российской Федерации от 29 июня 2015 г. №162-ФЗ "О стандартизации в Российской Федерации" (в ред. 03.07.2016 г.). Доступ из справ.-правовой системы полнотекстовой базы данных.
4. ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. М.: Стандартинформ, 2006. 16 с.
6. Мусаев А.А., Шерстюк Ю.М. Аналитические информационные технологии в управлении безопасностью промышленного предприятия. // Труды СПИИРАН. 2002. Вып. №1. Т.№2. С. 84 - 91.
7. Котенко И.В., Саенко И.Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах. // Труды СПИИРАН. 2013. Вып. №1(24). С. 21 - 40.
8. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. М. : Стандартинформ, 2014. 156 с.
9. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. М. : Стандартинформ, 2014. 145 с.
10. ГОСТ Р 53633.4-2015 Информационные технологии. Сеть управления электросвязью. Расширенная схема деятельности организации связи (eTOM). Декомпозиция и описания процессов. Процессы уровня 2 eTOM. Основная деятельность. Управление и эксплуатация услуг. М. : Стандартинформ, 2015. 8 с.
11. ГОСТ Р 53633.6-2012 Информационные технологии. Сеть управления электросвязью. Расширенная схема деятельности организации связи (eTOM). Декомпозиция и описания процессов. Процессы уровня 2 eTOM. Стратегия, инфраструктура и продукт. Разработка и управление услугами. М. : Стандартинформ, 2013. 8 с.
12. ГОСТ Р 53110-2008 Система обеспечения информационной безопасности сети связи общего пользования. Общие положения. М. : Стандартинформ, 2009. 20 с.
13. ГОСТ Р ИСО/МЭК 12207-2010 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств. М. : Стандартинформ, 2011. 100 с.
14. J. Reason Human error: models and management. [сайт]. URL: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1117770/ (дата обращения: 15.10.2016).
15. Демидов А.А., Никифоров О.Г., Саенко И.Б. Разработка концепции обеспечения информационной безопасности информационно-телекоммуникационных систем органов государственной власти. // Труды СПИИРАН. 2012. Вып. №3(22). С. 71 - 83.
16. Журавель Е.П., Шерстюк Ю.М. Информационная безопасность в расширенной схеме деятельности организации связи. // Проблемы информационной безопасности. Компьютерные системы. 2016. № 2. С. 29 - 36.
17. Анфилатов В.С., Емельянов А.А., Кукушкин А.А. Системный анализ в управлении. Учебное пособие. / Под ред. Емельянова А.А. М. : Финансы и статистика, 2002. 368 с.
18. Руководство администратора шлюза однонаправленной передачи данных "З-Кросс" производства ООО "СиЭйЭн" [сайт]. URL: http://cansec.ru/uploads/support/manual_z_cross.pdf (дата обращения: 30.10.2016).

19. AlienVault's Open Source Security Information and Event Management product: [сайт]. URL: https://www.alienvault.com/products/ossim/ (дата обращения: 26.10.2016).
20. Бочков М.В., Журавель Е.П., Копчак Я.М., Паращук И.Б., Саенко И.Б. Патент на изобретение № 2296365. Устройствопоискаинформации. М. : ФИПС, 2007. 24 с.
21. Open and extensible LGPv3 deep packet inspection library: [сайт]. URL: http://www.ntop.org/products/deep-packet-inspection/ndpi/ (дата обращения: 26.10.2016).
22. Snort is a network intrusion detection & prevention system: [сайт]. URL: https://www.snort.org/downloads#snort (дата обращения: 26.10.2016).
23. ГОСТ Р ИСО/МЭК 27033-3-2014 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. М. : Стандартинформ, 2014. 36 с.

УДК 004.056.57

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ С ПРИМЕНЕНИЕМ НЕЙРОННЫХ СЕТЕЙ

Захаров Руслан Владимирович, Лаута Олег Сергеевич, Крибель Александр Михайлович, Дмитрий Владимирович Соловьев
Военная академия связи имени МаршалаСоветского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: vlasenko199@yandex.ru, asuetin5@yandex.ru

Аннотация. В работе представлен подход по обеспечению безопасности управления роботизированных систем на основе искусственного интеллекта с применением нейронных сетей.

Ключевые слова: *роботизированная система; искусственная нейронная сеть; метод преобразования.*

SAFETY OF MANAGEMENT OF ROBOTIC SYSTEMS ON THE BASIS OF ARTIFICIAL INTELLIGENCE WITH APPLICATION OF NEURAL NETWORKS

Zakharov Ruslan, Lauta Oleg, Kribel Aleksandr,Soloviov Dmitriy
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckystr., 3
e-mail: vlasenko199@yandex.ru, asuetin5@yandex.ru

Abstract. Approach on safety of management of robotic systems on the basis of artificial intelligence with application of neural networks is presented in article.

Keywords: *robotic system; neural network; transformation method.*

На текущем этапе развития технологий робототехнические комплексы (РТК) выполняют широкий спектр задач в различных областях деятельности человека. Отдельную нишу занимают РТК, выполняющие задачи специального назначения: военные РТК, РТК, обеспечивающие ликвидацию последствий чрезвычайных происшествий и других задач, связанных с риском для жизни человека.

Одной из важнейших задач при построении РТК как специального назначения, так и некоторых других типов, является обеспечение управления комплексом. Под управлением РТК понимается решение комплекса задач, связанных с адаптацией робота к кругу решаемых им задач, программированием движений, синтезом системы управления и её программного обеспечения [1, 2].

Наибольший интерес для решения задач, связанных с риском для жизни человека, представляют интерактивные системы управления, так как при решении сложных задач пока что избежать необходимости участия оператора избежать не удаётся. При этом, более перспективным методом интерактивного управления РТК является дистанционное беспроводное управление. Применение данного метода управления позволяет изолировать оператора от опасных для жизни факторов, а также обеспечить максимально мобильный процесс управления.

Важнейшим вопросом, при построении и использовании РТК специального назначения, а в особенности, РТК, применяемых силовыми структурами, является обеспечение защищённости канала управления комплексом. Получение злоумышленником передаваемых сведений, их подмена, искажение или подавление могут привести к различными негативным последствиям вплоть до гибели людей. Для обнаружения злоумышленника и противодействия ему предлагается использовать системы, контролирующие процесс обмена данными в процессе управления РТК и выполняющими обнаружение аномальной активности на основе анализа протоколов различных уровней.

Хорошо зарекомендовавшим себя подходом к решению подобных задач является использование искусственных нейронных сетей (ИНС). Процесс построения профиля нормального поведения в случае с нейронными сетями сводится к созданию обучающей выборки, состоящей из примеров, содержащих данные нормального обмена РТК с оператором, и дальнейшего обучения ИНС с использованием этих данных. Алгоритмы обучения, обычно, выбираются на основе выбранного типа ИНС. Параметры ИНС выбираются эмпирическим путём в зависимости от конкретной задачи [3].В случае, когда профиль нормального поведения строится на основе данных

протоколов передачи, в качестве характеристик используются поля заголовков пакетов, а также дополнительные данные, такие как, например, временная метка, если эти данные не предусмотрены протоколом, но

Результатом работы такой ИНС является формирование топологической структуры (карты) [4], которая классифицирует входные примеры на кластеры (группы схожих примеров) и визуально отображает многомерные входные данные на плоскости нейронов. Важным преимуществом данного подхода является то, что эта ИНС является самообучающейся, то есть для обучения ей не нужны наборы входных данных и соответствующих им «правильных» выходных данных.

Таким образом, для идентификации аномальной активности по результатам работы оператору РТК следует дождаться формирования устоявшейся структуры кластеров на выходе ИНС, а в процессе дальнейшего функционирования РТК наблюдать за изменением данной структуры [5]. Наличие явных изменений в ней будет свидетельствовать об аномальном поведении. Задача прогнозирования в контексте обнаружения аномалий управления РТК будет заключаться в определении возможной следующей команды на основе информации о предыдущих. Если полученная команда будет значительно отличаться от прогнозируемых, то можно сделать вывод об аномальном поведении.

СПИСОК ЛИТЕРАТУРЫ

1. Елисеев А.И., Долгов А.А., Хорохорин М.А., Лаута О.С., Набатов К.А. Обеспечение живучести информационных систем (часть 3. Методы обеспечения и повышения живучести). Вестник Воронежского института ФСИН России. 2013. №1. С.91-94.
2. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П.Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 83-89.
3. Баранов В.В., Крибель А.М., Лаута О.С., Нечепуренко А.П. Применение метода топологического преобразования стохастических сетей для оценки эффективности средств защиты. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 47-52.
4. Коцыняк М.А., Карганов В.В., Лаута О.С., Нечепуренко А.П. Методика обоснования мер противодействия радиолокационной разведке высокоточного оружия. Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. № 9-10 (99-100). С. 54-57.
5. Баранов В.В., Гудков М.А., Крибель А.М., Лаута О.С., Нечепуренко А.П. Защита канала управления роботизированных систем. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 32-37.
6. Анисимов В. В., Бегаев А. Н., Стародубцев Ю. И. Модель функционирования сети связи с неизвестным уровнем доверия и оценки её возможностей по предоставлению услуги VPN с заданным качеством // Вопросы кибербезопасности. — 2017. — № 1(19). — С. 6–15.

УДК621.391(075.8)

АНАЛИЗ ТЕНДЕНЦИЙ ПРИМЕНЕНИЯ И ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ ХРАНЕНИЯ ДАННЫХ ДЛЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Зияев Павел Викторович[1], Паращук Игорь Борисович[2], Ткаченко Владимир Владиславович[1]
[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mails: shchuk@rambler.ru, U-429@inbox.ru

Аннотация. Проведен анализ реализуемых и перспективных подходов кприменению различных типов систем хранения данных в интересах некоторых видов облачных решений: для общедоступных (публичных) облаков, частных облаков и персональных (личных) облачных систем. Проанализированы вопросы информационной безопасности, требующие решения для систем хранения данных в рамках облачных технологий.

Ключевые слова: *система хранения данных; облачные решения; информационная безопасность; цифровые ресурсы хранения; технологии.*

ANALYSIS OF APPLICATION TRENDS AND ISSUES OF SECURITY OF INFORMATION SYSTEMS OF DATA STORAGE FOR CLOUD TECHNOLOGIES

Ziyaev Pavel[1], Parashchuk Igor[2], Tkachenko Vladimir[1]
[1]Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
[2] St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
e-mails: shchuk@rambler.ru, U-429@inbox.ru

Abstract. The analysis of realized and perspective approaches to application of various types of data storage systems in the interests of certain types of cloud solutions is carried out: for public clouds, private clouds and personal cloud systems. The issues of information security, which require solutions for data storage systems in the framework of cloud technologies, are analyzed.

Keywords: *storage system; cloud solutions; information security; digital storage resources; technologies.*

Известно, что в мире возрастает интерес к современным устройствам и системам хранения данных (СХД), причем увеличение спроса на цифровые ресурсы хранения обусловлено созданием взаимосвязанных, так называемых, «экосистем» данных. Это системы появились как следствие выхода на рынок телекоммуникаций и информационных технологий (ИТ) облачных вычислений, послуживших импульсом к развитию таких концептуальных инженерных решений, как ориентирование ИТ на потребителя, большие данные и мобильность предприятий [1, 2]. Отдельного рассмотрения, наряду с анализом перспектив применения таких систем, требуют вопросы их информационной безопасности, поскольку, с точки зрения защиты информации, облачные технологии вызывают неоднозначную реакцию у множества экспертов [3].

Как и с точки зрения безопасности информации, отношение к технологическим облачным решениям по хранению данных неоднозначное, еще недавно считалось, что облака представляют угрозу для традиционных технологий хранения данных.

Практика показывает, что эти опасения были напрасными, поскольку до сих пор востребованы и жесткие диски (HDD) и твердотельные накопители (SSD), используемые в облачных СХД. Активно используются разнообразные комбинации высокопроизводительных и недорогих решений по хранению данных, при необходимости организации, предприятия и провайдеры телекоммуникационных услуг пытаются обеспечить плавный перехода с одного решения на другое.

Современными тенденциями являются использование решений с кэшированием, например, двойных накопителей (систем, содержащих и SSD, и жесткий диск), внедрение систем хранения данных на базе SSD, дополняющих решения с жесткими дисками [1].

Проанализируем тенденции применения некоторых типов СХД для различных видов облачных решений: для общедоступных (публичных) облаков, частных облаков и персональных (личных) облачных систем [1, 2].

Что касается СХД в общедоступных облаках, используемых крупными предприятиями, то следует отметить, что наблюдаются высокие темпы их внедрения. При этом потенциал облака увеличивается пропорционально функциональной совместимости различных СХД, поэтому необходимо учитывать разнообразные варианты интеграции элементов СХД и возможность легкого осуществления миграцию с одной платформы хранения данных на другую.

Считается, что в общедоступных облаках в течение ближайших десяти лет аналитика и хранение больших данных станут ключевой технологической проблемой для СХД корпоративного класса. Вместе с тем, необходимость в надежном хранении и обеспечении безопасности информации на корпоративном уровне обуславливает необходимость реализации недорогих решений по хранению данных с высокой функциональной совместимостью, обеспечивающих надежность, скорость, отказоустойчивость и главное – защиту информации [3].

Поскольку облачные СХД продолжают развиваться, и далее будет востребованы различные типы устройств хранения, в том числе SSD – высокопроизводительные диски со скоростью вращения шпинделя 10 и 15 тысяч оборотов в минуту, а также диски самой большой емкости. При этом диски SSD обеспечивают более быструю и эффективную работу облака, что позволяет справляться с ускорением потоков данных без ущерба для безопасности информации.

Анализ СХД для частных облаков показывает, что потребность в цифровых системах хранения данных растет не только на уровне крупных предприятий, но и средних и малых организаций. Это обусловило необходимость создания более эффективных решений, ориентированных, преимущественно, на функциональную совместимость, поскольку СХД небольших организаций обычно вмещают все больше различных операционных систем.

Здесь актуальным средством является сетевое устройство хранения данных (NAS), представляющее собой набор жестких дисков и присоединенных программ и служб. Благодаря развитию технологий NAS, наряду со значительным количеством добавленных функций, стало возможным использование высокопроизводительных серверов, способных эффективно обрабатывать растущее количество клиентских запросов. Применение NAS открывает доступ к большей емкости и более гибким функциям, предоставляют преимущества облачных вычислений, например, удаленный доступ к файлам через Web-браузер и возможность легко выполнять резервное копирование или миграцию файлов на вторичное устройство хранения.

Что касается персональных облачных СХД, то объем всего цифрового содержимого потребителей стимулирует потребности в повышенной емкости систем хранения (на конец 2016 года – до 4,1 Зеттабайт). Помимо этого, все устройства с камерами, такие как смартфоны и планшетные ПК, пользуются все большей популярностью, что создает все больший объем цифрового содержимого.

Именно поэтому автоматизированная синхронизация обретет важное значение для СХД потребительского класса, т. к. пользователи будут переходить с локальных систем хранения на

облачные. Вместе с тем, даже с ростом общедоступных облачных СХД, персональные (домашние) облачные СХД наверняка составят значительную часть персональных облаков.

Важно помнить, что домашние системы NAS имеют много функций, присущих NAS для частных облаков, благодаря чему, с их помощью вполне реально создать персональную облачную СХД на несколько терабайт.

Возрастающие требования к гибким и защищенным системам хранения являются многоплановыми, сейчас в любой отрасти, где применяются СХД, мало сформировать только дополнительные ресурсы для хранения, необходимо увеличивать показатели производительности, гибкости и безопасности. Организации любого уровня и любой профильной принадлежности нуждаются в платформах с гарантированной безопасностью, высокой функциональной совместимостью, способных, например, предоставлять возможность виртуализации или работы с большими данными. Облачные технологии играют и будут играть исключительную роль для эволюции СХД, поскольку наряду с обеспечением информационной безопасности, позволят осуществить реализацию современной концепции персонализированных вычислений.

СПИСОК ЛИТЕРАТУРЫ

1. Спрос на устройства хранения в мире взаимосвязанных данных. // Seagate and BlackArmor, 2015. // [Электронный ресурс]: http://www.seagate.com/ru/ru/tech-insights/demand-for-storage.html.
2. Отчетмаркетинговогоподразделения Seagate и IDC Worldwide Enterprise Storage for Public and Private Cloud 2011-2015. // [Электронныйресурс]: http://www.idc.com/getdoc.jsp.containerId=230283.
3. Авраменко В.С. Адаптивный контроль защищенности информации от несанкционированного доступа на основе информационных образов. // Проблемы информационной безопасности. Компьютерные системы. 2010. № 2. С. 45-49.

УДК 629.7

МЕТОД ИЗМЕРЕНИЯ ПАРАМЕТРОВ ИОНОСФЕРЫ ДЛЯ ОЦЕНКИ СВОЙСТВ И ХАРАКТЕРИСТИК СПУТНИКОВОЙ РАДИОСВЯЗИ

Зорин Владимир Андреевич, Корякин Денис Дмитриевич, Андреев Глеб Владимирович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: vas@mil.ru

Аннотация. В работе рассматриваются существующие физический и радиотехнический подходы исследования распространения радиосигналов в ионосфере Земли. Предложен гибридный метод мониторинга.

Ключевые слова: *ионосфера; спутниковая связь.*

METHOD OF MEASUREMENT OF IONOSPHERE PARAMETERS FOR ESTIMATION OF PROPERTIES AND CHARACTERISTICS OF SATELLITE RADIOCOMMUNICATION

Zorin Vladimir, Koryakin Denis, Andreev Gleb
S.M. Budjonny Military Academy of the Signal Corps,
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: vas@mil.ru

Abstract. In this article, the existing physical and radio engineering approaches to the study of propagation of radio signals in the Earth's ionosphere are considered. A hybrid method of monitoring is proposed.

Keywords: *ionosphere; satellite communication.*

В вопросе прохождения радиосигналов через ионосферу зачастую применяется физический подход [1], в этом случае первоначально изучается вопрос прохождения радиосигнала в среде электромагнитного колебания, представленного во временной области в гармоническом виде. Переход к сигналу в этом случае связан с учетом спектрального состава сигнала. Это требует больших вычислительных мощностей и не имеет желаемой для общего решения задачи наглядностью. Также, возникают сложности при использовании полученного решения для сигналов иных форм.

Параллельно в радиотехнике развивался другой подход.

В отличии от предыдущего, ему можно дать название системного [2]. В этом случае среда распространения заменяется некой эквивалентной системой, имеющей частотную $H(f)$ и импульсную $h(\tau)$ характеристики.

Тогда выходной сигнал такой системы будет определяется интегралом свертки сигнала, поступающего на вход с импульсной характеристикой системы. При применении такого метода, тем не менее, возникает трудность перехода к такой эквивалентной системе, обусловленная определением связи между механизмами прохождения радиосигнала в ионосфере от излучателя к приемнику и

характеристиками канала. Для решения этого вопроса имеет место применение гибридного подхода [2,3] В таком случае описание механизмов распространения электромагнитных колебаний определенной частоты от излучателя к приемнику дает физический подход. Решение такой задачи дает возможность синтеза эквивалентной системы, называемой радиоканалом, и определения ее импульсной и частотной характеристик с учетом случайного характера распространения.

В следствии чего, предложенный подход позволяет с общих позиций заниматься исследованием распространения сигналов в неоднородных средах.

Особенной важным в этом подходе является возможность получения решения более важной в представленной проблеме задачи - исследования системных характеристик радиоканала (эквивалентна системы).

В настоящее время развитие и применение гибридного подхода является актуальным направлением исследования распространения радиосигналов в ионосфере и других неоднородных средах. Составная часть гибридного подхода - физический метод исследования распространения ВЧ в ионосфере часто базируется на уравнении Гельмгольца (уравнении волнового типа).

Показатель преломления $n(\vec{r}, f, t, T)$ определяется с помощью свойств среды распространения радиосигнала - ионосферы и является зависимым от частоты сигнала, времени.

Существует ряд методов решения уравнения Гельмгольца. Все они приближенные. Наибольшее распространение получил метод геометрической оптики, когда механизм распространения волны от передатчика к приемнику описывается лучом.

В задачах, решаемых в данной работе, заданы пункты передачи и приема связного сигнала. Для уравнения Гельмгольца (дифференциального) это означает задание граничных условий, которое, как известно, приводит к дискретным решениям (многолучевости). Это могут быть лучи, приходящие в точку приема одним или несколькими скачками, нижним и верхним (луч Педерсена) лучами.

Магнитное поле Земли приводит к двойному лучепреломлению и возникновению магнитоионных лучей (обыкновенному и необыкновенному) [4,5]. Влияние магнитного поля особенно проявляется при КЗР.

Удобство использования лучевого подхода при рассмотрении распространения ВЧ сигналов в ионосфере привело к тому, что используемая терминология связана с лучами. Например – термин многолучевость, дискретная и диффузная многолучевость и т.п. Очевидно, что фаза волны находится исходя из профиля концентрации электронов. Поэтому физический метод связан с выбором такой модели среды, которая дает возможность оценивать концентрацию в любой заданной на земле точке для любого времени и времени года. Зачастую для этих целей используют модель IRI при аппроксимации, задаваемых значений электронной концентрации, сегментами парабол (квазипарабол - MQP аппроксимация).

Гибридный метод основывается на том факте, что распространение гармонического колебания по парциальному лучу приводит к смещению ее фазы (набегу) на $\varphi_j(f,T)$ и изменению амплитуды на $H_{0j}(f,T)$. Поэтому распространение ВЧ сигнала по лучам возможно заменить его распространением в многомерной системе (радиоканале) с множеством входов (по лучам) и одним выходом. При этом каждый парциальный тракт (вход) имеет свою ФЧХ и АЧХ. Учитывая изменения во времени среды распространения (перемещения уровня отражения или изменения интегральной вдоль луча концентрации электронов) получим, что ЧХ - $H(f,T)$ является также функцией времени Т, т.е. линейная система имеет переменные во времени параметры.

В результате проведенного исследования проанализированы плюсы и минусы используемых прежде физического и радиотехнического подходов исследования распространения радиосигналов в ионосфере Земли. Предложен гибридный метод мониторинга.

СПИСОК ЛИТЕРАТУРЫ

1. Гинзбург, В.Л. Распространение электромагнитных волн в плазме / В.Л. Гинзбург. – М.: Наука, 1967.
2. Иванов, В. А. Основы радиотехнических систем ДКМ диапазона / В. А. Иванов, Н. В. Рябова, В. В. Шумаев. – Йошкар-Ола, 1998. – 204 с.
3. Арманд, Н.А. Коррекция дисперсионных искажений широкополосных сигналов / Н.А. Арманд, В.А. Иванов // Тр.XXI Всерос. науч. конф. «Распространение радиоволн». – Йошкар-Ола, 2005, т.1, С.10-18.
4. Иванов В.А. Зондирование ионосферы и декаметровых каналов связи сложными радиосигналами // Вестник Марийского государственного технического университета. Сер.: Радиотехнические и инфокоммуникационные системы, 2010. № 1 (8). С. 3-37.
5. Аллин, И.В. Классификация пространственной фокусировки видеоимпульсов в плазме на основе теории катастроф / И.В. Аллин, А.С. Крюковский, Д.С. Лукин, Д.В. Растягаев //Нелинейный мир. - 2009. - Т.7. - № 10. - С. 727-739.

УДК 004.056.53

АСПЕКТЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИИVPN В КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУРАХ

Зубакин Владимир Валентинович, Кий Андрей Вячеславович, Морозов Иван Васильевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: kiyarmy@yandex.ru

Аннотация. Проведен анализ особенностей применения технологии VPN в критических инфраструктурах, рассмотрены общие требования к корпоративной VPN, вопросы планирования и проектирования VPN сети, а также ряд вопросов, требующих учета при развертывании VPN сети.

Ключевые слова: *критическая инфраструктура; информационная безопасность; технология VPN (VirtualPrivateNetwork).*

THE VPN TECHNOLOGY APPLICATION ASPECTS IN CRITICAL INFRASTRUCTURE

Zubakin Vladimir, Kiy Andrey, Morozov Ivan
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: kiyarmy@yandex.ru

Abstract. The facilities of VPN application in critical infrastructure are analyzed. Thecommon the requirements to corporate VPN are considered. Planning, designanddeploymentVPNnetworkareconcluded.

Keywords: *critical infrastructure; information security; VPN technology (Virtual Private Network).*

Устойчивое к различным воздействиям и бесперебойное функционирование критической информационной инфраструктуры (КИИ) в условиях постоянного повышения сложности, масштабов и скоординированности компьютерных атак является одним из национальных интересов Российской Федерации в области информационной безопасности [1].

Особенностями крупных территориально-распределенных КИИ являются: объединение информационных систем, отдельных локальных сетей и сайтов, а также удаленных пользователей с помощью глобальной сети «Интернет» и цифровых сетей связи; обслуживание большого количества разнородных пользователей, имеющих различные потребности в сервисах и разные степени доверия; наличие широкого спектра угроз безопасности, как со стороны удаленных пользователей, так и со стороны внешних источников.

Все эти особенности обусловливают необходимость построения «наложенных» на существующие сети виртуальных частных сетей VPN (Virtual Private Network), обеспечивающих безопасный удаленный доступ по открытым каналам связи и позволяющих сочетать требования безопасности к предоставляемым сервисам системы. Однако, для эффективного применения VPN технологии требуется решение ряда специальных задач, связанных с выбором структуры сети, организацией работы пользователей и сетей КИИ, обеспечением требуемого уровня защиты данных и требуемых характеристик передачи и обработки информации.

Для построения VPN предлагается широкий выбор архитектур - виртуальные каналы Frame Relay/ATM, IP-туннели с использованием технологий GRE или IPSec, MPLS на магистралях IP+ATM или Frame Relay/ATM, которые постоянно совершенствуются и развиваются. Современными тенденциями развития архитектуры VPN стали технологии безопасной передачи не только данных, но и голосовых сообщений, видеотрафика, решения по упрощению построения, настройки и масштабирования крупных сетей VPN, а также предложение новых услуг с помощью объединения разных технологий VPN [2].

Так при развитии конвергентных сетей одним из обязательных требований к существующим VPN является поддержка мультимедийного трафика (создание так называемого V3PN - Voice and Video-Enabled VPN). Это требование обусловлено распределенной структурой КИИ и широким перечнем услуг современных управленческих процессов.

Использование мультисервисных свойств VPN позволяет создавать удаленные элементы КИИ с безопасной интеграцией в информационную инфраструктуру голоса, видео и данных.

К оборудованию, поддерживающему данную функциональность, предъявляются требования не только по шифрованию, но и по поддержке качества сетевого обслуживания, режима групповой рассылки, характерного для мультимедиа-приложений, созданию различных топологий и возможности по обеспечению надежности соединений.

На применение VPN в КИИ оказывает существенное влияние ряд факторов:

– в данных инфраструктурах априори присутствует конфиденциальная информация, при этом часть информации является государственной тайной, что требует целого ряда организационных и технических мер защиты;

– критичным является не только факт хищения обрабатываемой информации, но и возможность ее несанкционированной модификации или уничтожения. Критичным в этих системах также становится вывод из строя системных средств на продолжительное время (в результате DOS-атак или иных программных воздействий);

– не всегда достаточная квалификация персонала КИИ в вопросах обеспечения информационной безопасности, наличие инсайдерских угроз, что существенно снижает эффективность защиты.

В связи с этим к корпоративной VPN предъявляется ряд общих требований [3,4]:

– все задачи администрирования VPN в КИИ должны решаться централизованно (в составе VPN-сети должен функционировать АРМ администратора безопасности);

– наличие жесткой политики безопасности, обязательной к выполнению всеми участниками информационного процесса, при этом обмен данными происходит в соответствии с матрицей доступа (для различных видов трафика);

– обеспечение подконтрольности работы сети и достоверная идентификация всех источников информации;

– шифрование виртуальных каналов должно осуществляться автоматически, ключ шифрования пользователя в случае компрометации не должен позволять нарушить конфиденциальность данных при их хищении.

Существует еще одно условие применения VPN. VPN-решения используют шифрование при передаче информации и относятся к криптосредствам. Это приводит к тому, что выбор VPN решений ограничен отечественными продуктами, так как импортные не имеют сертификатов ФСБ. Данное обстоятельство накладывает существенные ограничения на применение VPN в КИИ.

Для эффективного планирования и проектирования любой вычислительной сети нужно заранее просчитать и знать некоторые обязательные параметры сети. Это в полной мере относится и к виртуальным частным сетям.

Важное значение при планировании VPN-сети имеет структура сети, интенсивность нагрузки, генерируемой пользователями КИИ, а также полосы пропускания каналов от провайдера до пограничного узла (маршрутизатора) КИИ [5]. Связано это, во-первых, с необходимостью приобретения у провайдера канала связи определенной полосы пропускания, а также с выбором оборудования, на котором будет строится VPN.

Расчет требуемой полосы пропускания транспортной сети производится на основе анализа организационно-штатной структуры КИИ, анализа результатов использования пользователями приложений и служб при работе сети.

При этом анализируется использование канала каждой службой, пиковые и средние нагрузки на канал, с учетом обеспечения требуемой доступности информации и комфортной работы пользователей. Расчет полосы пропускания может производиться методом суммирования, где в качестве слагаемых выступают средние значения нагрузки по категориям пользователей, умноженные на количество пользователей в категории.

Вышеприведенная методика расчета не дает нам никаких параметров качества обслуживания, которые необходимы, чтобы понять на сколько правильно и качественно спроектирована сеть VPN.

Проведя расчеты, основанные на аппарате теории массового обслуживания, можно произвести оптимизацию полученной необходимой пропускной способности канала, а также убедиться в обеспечении требуемого качества обслуживания проектируемой VPN-сети. При этом пограничный маршрутизатор рассматривается как одноканальная система с неограниченной очередью, так как все потоки данных проходят только через него по одному каналу [6].

В результате проведения расчетов можно определить среднее время обслуживания пакета и среднее время ожидания в очереди, на основании которых выбрать пограничный маршрутизатор с требуемыми характеристиками, а также произвести оптимизацию пропускной способности канала, то есть снизить до такого значения, при котором время ожидания в очереди не будет превышать время обслуживания.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ от 05.12.2016.
2. Росляков, А. В. Виртуальные частные сети. Теория и практика применения / А. В. Росляков. - М.: Эко-Трендз, 2007. - 304 с.
3. Щеглов А.Ю. «Корпоративная VPN. Требования к построению и подходы к упрощению администрирования». Сайт ITSec.Ru-2007.
4. Баранов В.В., Бирюков М.А., Кравченко С.А., Максимов А.С., Саенко И.Б. Имитационная модель для анализа рисков информационной безопасности при проектировании ролевых схем разграничения доступа к базам данных // Актуальные проблемы обеспечения информационной безопасности. Труды межвузовской научно-практической конференции. 2017. С. 26-31.
5. Вентцель Е. С., Овчаров Л. А. Теория вероятностей. М., 1969, 368 с.
6. Агеев С.А., Шерстюк Ю.М., Саенко И.Б., Полубелова О.В. Концептуальные основы автоматизации управления защищенными мультисервисными сетями // Проблемы информационной безопасности. Компьютерные системы. 2011. № 3 С. 30-39.

УДК 004.7

ПОСТАНОВКА ЗАДАЧИ НАХОЖДЕНИЯ МЕСТОРАСПОЛОЖЕНИЯ КОНТРОЛЛЕРА НА ПРОГРАММНО-КОНФИГУРИРУЕМОЙ СЕТИ

Зубакин Владимир Валентинович, Хмелляр Николай Александрович,
Шинкарев Семен Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: theboyxxx@yandex.ru

Аннотация. На сегодняшний день состояние телекоммуникационных сетей показывает, что возможности традиционных технологий близки к исчерпанию. Возможным вариантом решения возникающих проблем является переход на концепцию программно-конфигурируемых сетей. Данный подход предлагает разделить уровень управления и уровень передачи данных путем выноса функций управления на отдельное устройство (контроллер). Для этого необходимо решение ряда возникающих задач, одной из которых является нахождение месторасположения контроллера на сети.

Ключевые слова: *программно-конфигурируемые сети; ПКС; сети связи специального назначения.*

STATEMENT OF THE PROBLEM POSITIONING CONTROLLER ON SOFTWARE DEFINED NETWORKING

Zubakin Vladimir, Hmellyar Nikolai, Shinkarev Semyon
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: theboyxxx@yandex.ru

Abstract. To date, the state of telecommunication networks shows that the capabilities of traditional technologies are close to exhaustion. Possible solution to the emerging problems is the transition to the concept of software defined networking. This approach proposes to separate the management level and the level of data transmission by allocating control functions into a single device (controller). This requires the solution of a number of emerging challenges, one of which is finding the location of the controller on the network.

Keywords: *software defined networks; SDN; special purpose communication networks.*

Первоочередными задачами сетей связи специального назначения является обеспечение устойчивой связи в интересах обороны страны, безопасности государства и его населения, органов государственного управления, как в мирное, так и в военное время. Для решения этих задачи необходимо, чтобы сети связи обладали достаточной пропускной способностью и производительностью.

На текущий момент выделяет две основные проблемы построения традиционных сетей специального назначения:

1. Резкий рост объемов передаваемого трафика.
2. Усложнение управления сетью

Возможным вариантом решения указанных выше проблем является переход на концепцию программно-конфигурируемых сетей.

Программно-конфигурируемая сеть (ПКС) – это новый подход к построению архитектуры сетей связи, при котором уровень управления сетью и уровень передачи данных разделяются за счет переноса функций на отдельное центральное устройство, называемое контроллером [1].

По сравнению с традиционными сетями, данный подход дает следующие преимущества:

1. Программируемость и гибкость управления сетью, упрощение управления сетью и ее модификации за счет создания новых приложений или изменения существующих, автоматизация управления сетями.
2. Адаптивность управления сетью, возможность изменять состояние сети в режиме реального времени с учетом изменяющихся условий функционирования.
3. Упрощение структуры и логики сетевых устройств, поскольку теперь им не требуется обрабатывать огромное количество стандартов и протоколов, а достаточно выполнять только инструкции, полученные от контроллера.
4. Снижение стоимости сетевой инфраструктуры в целом, связанное с удешевлением модернизации системы и уменьшением энергопотребления [2].

Основой концепции ПКС является:

1. разделение процессов передачи и управления данными (за счет снятия с коммутаторов нагрузки по управлению данными эти устройства направят все свои мощности на ускорение перемещения трафика, что повысит производительность);

2. единый, унифицированный, независящий от поставщика интерфейс между уровнем управления и уровнем передачи данных (при использовании протокола взаимодействия между сетевыми устройствами и программно-конфигурируемой сети решается проблема зависимости от сетевого оборудования какого-либо конкретного поставщика, поскольку используется общие абстракции для пересылки пакетов, которые сетевая операционная система использует для управления сетевыми коммутаторами);

3. логически централизованное управление сетью, осуществляемое с помощью контроллера с установленной сетевой операционной системой и реализованными поверх сетевыми приложениями (логически-централизованное управление данными в сети предполагает вынесение всех функций управления сетью на отдельный физический сервер, называемый контроллером, который находится в ведении администратора сети).

Таким образом, концепция ПКС для построения сетей связи специального назначения (СССН) является перспективным направлением в развитии сетевых технологий. Использование данного подхода позволит повысить производительность и масштабируемость сетей, упростить управления и снизить затраты на оборудование и сетевые приложения.

Для построения сети связи специального назначения как программно-конфигурируемой сети необходимо решения ряда задач, одной из которых является нахождения месторасположения контроллера на сети. Структуру сети связи можно представить в виде графа G = (V, E, S, C, P), где V это множество элементов сети, где V1 – коммутаторы, V2 – контроллер или контроллеры, в случае если есть необходимость повысить устойчивость подсистемы управления сети связи специального назначения, E – множество ребер (линий/каналов связи), S – вектор устойчивости структурной сети, C – качество цифровых каналов, P – приведенная стоимость (протяженность линий и количество элементов сети) [3].

Задачу месторасположения контроллера на сети можно свети к задаче нахождения центра графа, где необходимо учесть: устойчивость каждой линии связи, количество переходов от конечного коммутатора до контроллера (количество хопов) и ряд других требований.

Как известно, центр графа возможно определить через нахождение диаметра, эксцентриситета и радиуса сети [4], где центром будет является вершины с минимальным радиусом.

Для решения задачи нахождения местоположения контролера можно воспользоваться алгоритмом Флойда-Уоршелла, в основе которого лежит преобразование структурной матрицы размером V×V, где элементы матрицы весовые коэффициенты ребер графа. Достоинством данного алгоритма является простата реализации и возможность учесть любую метрику.

Таким образом, решение задачи нахождения месторасположения контроллера сводится к выбору метрики позволяющий учесть различные требования и показатели, влияющие на целевые функции.

СПИСОК ЛИТЕРАТУРЫ

1. Коломеец А. Е., Сурков Л. В. «Программно-конфигурируемые сети на базе протокола OpenFlow» // Инженерный вестник 05.05.14 С. 519 – 524
2. Бойко А. П., Буланов М. С., Шинкарев С. А. «Постановка задачи синтеза потоковой структуры транспортной сети связи специального назначения и варианты ее решения» // Сборник научных статей СПбГПУ. Ч. 1. – СПб. 2014. С. 66 – 69
3. http://www.osp.ru/ (дата обращения 24.10.16)
4. Новиков Ф. А. Дискретная математика для программистов: Учебник для вузов. 3-е изд. — СПб.: Питер, 2009. С. 285 – 286

УДК 004.7; 004.49.5

МОДЕЛЬ НАРУШИТЕЛЯ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ АБДУКТИВНОГО СИНТЕЗА СТРУКТУР СЦЕНАРИЕВ

Карганов Виталий Вячеславович, Липатников Валерий Алексеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: vitalik210277@mail.ru, lipatnikovanl@mail.ru

Аннотация. Работа посвящена применению интеллектуальных агентов для управления информационной безопасности организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией. Инструментом решения, является применение способности к абдуктивному порождению новых знаний, основанной на выводах по аналогии.

Ключевые слова: *информационно-вычислительная сеть; интеллектуальный агент; система массового обслуживания; система знаний; гиромат.*

MODEL OF THE INFRINGER IN PROVIDING INFORMATION SECURITY BASED ON ABDUCTIVE SYNTHESIS OF STRUCTURES OF SCENARIOS

KarganovVitaly, LipatnikovValery
[1]Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: vitalik210277@mail.ru,lipatnikovanl@mail.ru

Abstract. The article is devoted to the use of intelligent agents for managing the information security organization integrated structures based on a dedicated server with container virtualization. The solution tool is the use of abductive ability to produce new knowledge based on conclusions by analogy.

Keywords: *computer information network; intelligent agent; queueing system; system knowledge; giromat.*

В настоящее время, необходим поиск решений по анализу и прогнозированию действий нарушителя для проактивного управления информационной безопасностью (ИБ) информационно-вычислительной сети (ИВС). Для решения задач анализа поведения нарушителя, осуществляющего несанкционированное воздействие на функционирование масштабируемой ИВС применяется аппарат теории массового обслуживания [1].

Решение. Предполагается применение интеллектуальных агентов (ИА) для управления ИБ организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией. ИА должны учитывать знания о стратегиях действий нарушителя в виде модели. Под ИА понимается любая физическая или виртуальная единица, способная осуществлять действие на других агентов и на самих себя, общаться с другими агентами, воспринимать среду, прогнозировать изменения среды и обладать способностями к обучению.

Важнейшей особенностью ИА является способность функционировать в условиях неточной, нечеткой и противоречивой информации. Модель агента включает систему восприятия и первичную обработку информации (рецепторы), блок памяти, процессор, эффекторы. Блок памяти состоит из системы фильтров, обеспечивающих выделение наиболее значимой для агента информации, внутренней модели внешнего мира и модели самого агента. Процессор обеспечивает объединение и переработку разнородных данных, принятие решений о выполнении тех или иных действий. Эффекторы выполняют функцию воздействия на среду.

Необходимо наделить систему ИА способностью к абдуктивному порождению новых знаний, основанному на выводах по аналогии. Настоящая способность, имеет широкое поле научного и прикладного использования, в том числе, в системах искусственного интеллекта. При этом стоит также отметить, что абдуктивные рассуждения чаще всего используются для открытия эмпирических законов, которые устанавливают необходимые регулярные связи между наблюдаемыми свойствами и отношениями явлений. Отсюда следует, что, обладая указанной способностью, система ИА сможет обучаться на прецедентах, имеющих место в различных проблемных областях, перенося знания о явлениях, наблюдаемых в одной проблемной области, в другую. При этом важным является тот факт, что, исходя из решаемой задачи, установление аналогий может осуществляться путем нахождения подобных структур, инвариантных свойств и близких действий, описанных в системе знаний.

Рассматривая последовательность действий, как систему массового обслуживания, можно выделить в качестве исходных данных поступление заявок и их выполнение. Где в качестве заявок принят поток требований на осуществление компрометации системы защиты: проведение пассивного мониторинга; активного мониторинга, преодоления системы защиты ИВС. Чтобы обеспечить возможность синтеза гироматом сценариев упреждающего поведения в конфликте, может оказаться весьма полезным механизм абдуктивного порождения новых знаний, основанный на выводах по аналогии.

Гиромат создаётся для достижения целей и по природе своей является образованием, предназначенным для поиска нового устойчивого состояния на более высоком эволюционном уровне, реализуя для этого негэнтропийный процесс [2]. В процессе своего функционирования гиромат строит в своей памяти модель окружающей среды и синтезирует программу действий в соответствии с заложенными в него целями, сообразуясь с этой моделью. Основной моделей сознания и самосознания гиромата служит специальный модельный язык, позволяющий имеющимися в нем средствами отображать структурно-функциональные взаимоотношения в среде, гиромате и между средой и гироматом. С помощью модельного языка в памяти гиромата строится система моделей, связанных между собой сложными функциональными связями.

В процессе накопления жизненного опыта гиромат с помощью модели кратковременных гипотез формирует некоторые устойчивые закономерности, обнаруживаемые им в окружающей среде и в своей структуре. Эти гипотезы относятся к устойчивости отображений, скорости и частоте смены. Также необходимо отметить, что если в среде помимо гиромата функционируют другие устройства, интересы которых пересекаются с его интересами, то возникает конфликтная ситуация, и гиромат при выработке своих решений вынужден учитывать возможные действия других активных устройств. В этом случае гиромат использует специальную модель активной среды, в которой рефлексивно отражает возможность действия своих конкурентов и схему их рассуждений при принятии решений.

Применение способа моделирования обеспечит при проактивном управлении ИБ реализовать адаптацию к окружающей среде, а поиск и усвоение удачных бифуркаций. Где их знание позволит существенно облегчить исследование реальных рассматриваемых систем, а именно предсказать характер оригинальных решений (направлений), возникающих в момент перехода системы в качественно другое состояние. Оценить их достоверность и устойчивость при решении задач анализа

поведения нарушителя, осуществляющего несанкционированное воздействие на функционирование масштабируемой ИВС.

СПИСОК ЛИТЕРАТУРЫ

1. Липатников, В. А. Метод управления безопасностью информационно-вычислительных сетей на основе выделенного сервера с контейнерной виртуализацией / В.А. Липатников, А.А. Шевченко, А.Д. Яцкин // Информационные системы и технологии. № 4 (102). 2017. С.116-126.
2. Поспелов Д.А. Ситуационное управление: теория и практика. М.: Наука. –Гл.ред.физ.-мат.лит., 1986. – 288с.

УДК 65.011.56

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ

Карпов Александр Владимирович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: a.kar1986@yandex.ru

Аннотация. В докладе проведен анализ источников угроз на объекте информатизации, их выявление и определение степени опасности каждой из них с помощью логико-вероятностной теории безопасности и риска, являющейся важным инструментом для построения модели угроз безопасности информации на объекте информатизации.

Ключевые слова: *информация; объект информатизации; безопасность информации; логико-вероятностная теория.*

MODEL OF THREATS TO INFORMATION SECURITI AT THE OBJEKT OF INFORMATIZAZION

Karpov Aleksander
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckystr., 3
e-mail:a.kar1986@yandex.ru

Abstract. The report analyzes the sources of threats on the object of informatization, their identification and determination of the degree of danger of each of them using the logical-probabilistic theory of safety and risk, which is an important tool for the construction of the model security threats information on the object of informatization.

Keywords: *information; informatization object; security of information; logical-probabilistic theory.*

Информация в современном мире является крайне важным ресурсом и инструментом, и в нашем веке информационных технологий она играет очень важную роль. Неправомерное искажение или фальсификация, любое повреждение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах наносят серьезный материальный и моральный урон многим субъектам, участвующим в процессах автоматизированного информационного взаимодействия.

Защита информации на объекте информатизации (ОИ) достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от утечки по техническим каналам, несанкционированного доступа, программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также работоспособности технических средств.

На объекте информатизации защите подлежит речевая информация и информация, обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

Значимость рассматриваемого вопроса подчеркивается тем обстоятельством, что надежную и эффективную систему обеспечения безопасности информации можно создать только при надлежащем учете всех возможных угроз. Если хоть одна из угроз упущена, то система обеспечения безопасности информации в целом будет не эффективной [1].

Как правило, выделяют следующие источники угроз на объекте информатизации:

- иностранные разведки и спецслужбы;
- промышленный шпионаж;
- преступные группы и элементы;
- стихийные бедствия и катастрофы;
- неправомерные действия руководства и государственных структур;
- ошибки и непреднамеренные действия персонала;
- неисправности оборудования и программного обеспечения;
- преднамеренные действия персонала.

В настоящее время существует две группы путей или способов реализации угроз. К первой группе относятся угрозы, реализуемые без проникновения на охраняемую территорию и без доступа к информационной системе: анализ открытой информации; применение дистанционных средств разведки; анализ поставок, продукции, отходов; дистанционное внедрение закладных устройств.

Кроме того, могут реализовываться угрозы с проникновением на охраняемую территорию или с получением доступа к информационной системе. К этой группе относятся: непосредственная установка закладок; прямое копирование, уничтожение, хищение физического носителя или документа; применение программно-технических воздействий; несанкционированный доступ к информационным ресурсам; порча оборудования.

Научный подход к проблеме безопасности информации (БИ) требует проведения комплексного анализа, классификации угроз, основных поражающих и влияющих факторов, поведения окружающей среды и действий персонала. Для решения этих вопросов необходимы соответствующие методы математического моделирования [2].

Модель угроз безопасности информации на ОИ необходима для анализа уязвимостей в системе защиты информации и выявления угроз БИ. Выявление угроз БИ и их ранжирование возможно с помощью логико-вероятностной (ЛВ) теории безопасности и риска, где под степенью риска в данном случае будем понимать вероятность реализации угрозы нарушения БИ на ОИ.

ЛВ-теория безопасности и риска позволяет моделировать и анализировать риск в системах, элементы которых имеют несколько состояний, и применять ЛВ-модели для количественного моделирования и анализа риска в различных системах. ЛВ-модель безопасности и риска позволяет осуществлять активное сценарное управление риском неуспеха в сложных системах на стадиях проектирования, испытаний и эксплуатации на основе анализа риска [3].

Фундаментальными понятиями в ЛВ-теории безопасности и риска являются понятие опасного состояния системы (в нашем случае это угроза нарушения БИ на ОИ), характеризующегося ущербом различного масштаба, и понятие опасности – способности системы переходить в опасное состояние.

В каждом конкретном случае необходимо дать аналитическое описание этого опасного состояния системы, которое может привести к нарушению БИ на ОИ. В ЛВ-теории безопасности и риска такое описание начинается с составления сценария опасного состояния, которое осуществляется с помощью конъюнкций и дизъюнкций инициирующих событий и условий. В качестве таковых выступают различные внешние и внутренние воздействия, приводящих к нарушению БИ на ОИ.

Далее осуществляется переход от логической функции риска к вероятностной функции риска, что крайне необходимо для оценки угроз БИ и их роли в создании опасного состояния системы, приводящего к нарушению БИ на ОИ. Данный переход осуществляется путем ортогонализации Л-функции риска, записанной в дизъюнктивной нормальной форме (ДНФ). Ортогонализация Л-функции возможно многими методами, некоторыми из которых являются метод прямой ортогонализации и метод условных вероятностей.

На основе логических и расчетных вероятностных моделей определяются значения показателей свойств или риска безопасного функционирования объекта и реализуются различные методики выработки и обоснования управленческих решений, исключающих нарушение безопасности информации на объекте информатизации.

СПИСОК ЛИТЕРАТУРЫ

1. Алашеев В.В., Ерышев В.Г., Никифоров О.Г., Демидов А.А. К формированию модели угроз защищенности информации на объектах информатизации от утечки по техническим каналам. Защита информации. Инсайд, №3, 2011, — с.92.
2. Лепешкин О.М., Орловский В.М. Развитие математического аппарата информационной безопасности. Известия ЮФУ. Технические науки, № 4 (33), 2003, — с.91-92.
3. Соложенцев Е.Д. Сценарное логико-вероятностное управление риском в бизнесе и технике. Издательский дом «Бизнес-пресса», 2006, — с.218-228.

УДК 65.011.56

ПОДХОДЫ К СОВЕРШЕНСТВОВАНИЮ СИСТЕМЫ КОНТРОЛЯ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТЕ УПРАВЛЕНИЯ

Карпов Александр Владимирович, Лепешкин Олег Михайлович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: a.kar1986@yandex.ru

Аннотация. В докладе проведен анализ и рассмотрены вопросы функционирования существующей системы контроля состояния защиты информации на объекте управления, актуальность развития системы контроля защищенности в целях повышения эффективности системы защиты противостоять широкому спектру угроз.

Ключевые слова: *система защиты информации; контроль защищенности; техническая разведка; объект управления.*

APPROACHES TO IMPROVING THE SYSTEM FOR MONITORING THE STATE OF INFORMATION SECURITI AT THE CONTROL SITE

Karpov Aleksander, Lepeshkin Oleg
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckystr., 3
e-mail:a.kar1986@yandex.ru

Abstract. The report analyzes and discusses the functioning of the existing system for monitoring the state of information security at the management site, the urgency of developing security monitoring system in order to increase the effectiveness of the protection system to withstand a wide range of threats.

Keywords: *information security system; security monitoring; technical intelligence; control object.*

Система защиты информации любого объекта контроля включает в себя подсистему управления защитой (вкл. организационные мероприятия и технические меры), подсистему принятия решения и подсистему контроля состояния защиты (вкл. организационный контроль и технический контроль эффективности и надежности принимаемых мер, являющийся неотъемлемой частью защиты скрываемых объектов и информации от технических средств разведки (ТСР) [1].

В условиях совершенствования средств информационного противоборства, стратегии применения средств защиты должны предусматривать оптимальное организационное управление механизмами защиты, под которым понимают процесс целенаправленного воздействия на средства и механизмы защиты информации для организации эффективного их применения по назначению. Данное требование достигается интеграцией перечисленных подсистем и качественным их функционированием в комплексе [2].

Для качественной и эффективной защиты от ТСР и действий нарушителя (незаконных формирований и т.д.) в каждом конкретном случае необходимо проводить тщательный анализ сведений о скрываемых объектах и учитывать возможность их проявления через соответствующие демаскирующие признаки (ДП). Поэтому так важно выявление источников информации для ТСР, анализ ДП скрываемых объектов и возможных каналов утечки информации [3].

Основной недостаток существующей системы защиты – попытка достичь требуемого уровня безопасности информации, применив отдельные методы и средства защиты без их увязки в единую систему защиты информации. Традиционно подсистема контроля не стала полноценно взаимосвязанной составляющей, а функционирует в значительной степени самостоятельно.

В настоящее время вне зависимости от принадлежности объектов контроля к тому или иному ведомству (ФСБ, ФСО, МО, МЧС и т.д.), контроль защищенности осуществляется пообъектово, т.е. каждый объект контролируется отдельно, зачастую без учета особенностей его работы. Имеет место явно выраженное противоречие, заключающееся, с одной стороны в системности ведения иностранными государствами всесторонней комплексной разведки и, с другой стороны, организация и сосредоточение усилий на защите отдельных средств и процессов, а не комплексных объектов в целом. Причем, при выявлении органом контроля фактов нарушения радиоэлектронной обстановки объекта, информация независимо от других передается по инстанции того ведомства, в ведении которого находится данный объект. Доведение данных, полученных средствами контроля, до органов обработки и принятия решения, осуществляется в масштабе времени, далеком от реального. Также необходимо отметить, что вне зависимости от принадлежности, объект контроля, рабочие состояния которого неизменны, либо изменяются в пределах допустимого, контролируется с применением тех же сил и средств контроля, что и объект, состояние которого динамично меняется (работа - сбой функционирования - восстановление работоспособности и т.д.). Каждый объект защиты имеет различную важность и для каждого из них существует свое допустимое время ведения контроля (как сумма времени на обнаружение нарушения ограничений и времени их пресечения). Таким образом, в ряде случаев возникает тенденция несоответствия объема сил и средств контроля защищенности реальным потребностям объекта с учетом специфики его функционирования.

Тенденция постоянного совершенствования средств технической разведки (ТР) привело к тому, что появилась возможность быстро и скрытно перенацеливать средства добывания с объекта на объект в больших регионах, а органам обработки – использовать при автоматизированной обработке ранее накопленные сведения. Совокупность независимых разведданных объединилась в целостную многомерно-связанную интеграцию сведений обо всей группировке объектов. Ее многомерная инфраструктура стала результатом отслеживания средствами разведки разнородных связей (пространственных, временных, структурных и функциональных) между объектами [3].

На основании вышеизложенного следует вывод, что основным требованиям к мероприятиям контроля, таким как всесторонность, своевременность и достоверность, существующая система

контроля в полной мере не удовлетворяет и требует перехода на качественно новый уровень информационного обеспечения органов военного управления по результатам контроля защищенности.

Таким образом, из анализа особенностей существующей системы контроля можно сделать вывод о том, что это сложная система с управлением, которая должна управляться органами контроля в динамике.Решаемые системой контроля задачи в первую очередь должны обеспечивать реализацию следующих основных функций: контроля, анализа, учета и прогнозирования.

Контроль защищенности объекта контроля заключается в выявлении отклонений между плановыми (нормативными) и фактическими показателями его функционирования, а также в выявлении причин обнаруженных отклонений. Результаты контроля защищенности необходимы для своевременного принятия решений по корректировке режимов эксплуатации объекта контроля в целях сохранения высокой эффективности его функционирования (обеспечения живучести, электромагнитной совместимости радиоэлектронных средств и систем государственного управления и т.д.).

Анализ заключается в исследовании всего множества факторов, характеризующих состояние и особенности функционирования объекта контроля в настоящее время и в некоторый заданный период с целью выявления скрытых закономерностей его развития.

Учет заключается в сборе, фиксации и накоплении информации о состоянии объекта контроля. На основании учетных данных уточняется текущее состояние объекта, а также прогнозируется его поведение в будущем. Учет состояний объектов и динамики их изменения ведется в соответствующей базе данных.Внесение изменений в базе данных (БД) должно производиться по мере поступления информации об изменениях, произошедших на объекте в соответствии со сложившейся обстановкой и требованиями действующих нормативных документов. Периодичность внесения изменений в БД может колебаться от нескольких минут (секунд) до нескольких месяцев. Поступающие сведения сопровождаются временными метками (дата и время смены состояния или режима использования) и, при необходимости, причины этого изменения. В системе контроля защищенности собирается информация о состоянии и аномалиях на объектах контроля, которая обрабатывается должностными лицами органа контроля, а затем формируются решения по коррекции состояния этих объектов и доводятся до должностных лиц этих объектов.

Прогнозирование представляет собой определение тенденций изменения значений показателей функционирования (состояний) объекта контроля на ближайшую перспективу, а в существующей системе контроля отсутствует паспортизация объектов контроля, отражающая историю их разведзащищенности от начала функционирования до текущего момента. В результате чего, ввиду отсутствия данных о динамике изменения демаскирующих признаков объекта контроля с течением времени, прогнозирование состояний функционирования последнего не представляется возможным.

Заключение. Организация и обеспечение эффективной защиты требует достоверных данных о состоянии защищаемого объекта и необходимости системного и комплексного подхода к его защите и информации, обрабатываемой на нем. Текущий контроль (в реальном или близком к реальному масштабах времени) защищенности объекта контроля позволяет повысить эффективность системы защиты противостоять широкому спектру угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Карпов А.В., Худайназаров Ю.К., Репников А.Ю. Современные задачи радиомониторинга. Сборник трудов всеармейской научно-практической конференции «Инновационная деятельность в Вооруженных Силах Российской Федерации», —2016, — с.266-270.
2. Корсунский А.С., Лепешкин О.М. Подход к формализации автоматизированной информационной системы для оценки функциональной безопасности // Вопросы радиоэлектроники. — 2012, — Т.3, №1. с.75-82.
3. Меньшаков Ю.К. Теоретические основы технических разведок: Учеб. пособие / Под ред. Ю.Н. Лаврухина. — М.: Изд-во МГТУ им. Н.Э. Баумана, — 2008, — с.7-11.

УДК 004.056.57

МЕТОДИКА ПРОГНОЗИРОВАНИЯ ПРОТОКОЛЬНЫХ ВОЗДЕЙСТВИЙ НА РОБОТИЗИРОВАННЫЕ СИСТЕМЫ

Коцыняк Михаил Антонович, Дементьев Владислав Евгеньевич, ТесляСергей Петрович, ЛаутаОлег Сергеевич
Военная академия связи имени Маршала Советского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: vlasenko199@yandex.ru, asuetin5@yandex.ru

Аннотация. В работе рассмотрен подход по прогнозированию протоколированных воздействий на роботизированные системы на основе метода двух функций.

Ключевые слова: *роботизированная система; канал управления; метод преобразования.*

TECHNIQUE OF FORECASTING OF LEGAL IMPACTS ON ROBOTIC SYSTEMS

Kocinyak Mikhail, Dementiev Vladislav, Teslya Sergei, Lauta Oleg
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckystr., 3
e-mail: vlasenko199@yandex.ru, asuetin5@yandex.ru

Abstract. In article approach on forecasting of the recorded impacts on robotic systems on the basis of a method of two functions is considered.

Keywords: *robotic system; control path; transformation method.*

Информация о сетевом трафике имеет статистический характер и представляет собой временные последовательности. Методы статистического анализа сетевого трафика широко освещены при их использовании в качестве инструментов прогнозирования загруженности каналов управления, определения потерь, качества управления и т.п. С точки зрения обеспечения сетевой безопасности, проводить анализ сетевого трафика крайне необходимо для решения задач сетевого администрирования, и мониторинга корректного функционирования роботизированных систем (РБС).

Как класс статистический анализ относится к поведенческим методам определения нарушений в каналах управления и основан на сопоставлении текущего состояния РБС с некими определенными заранее признаками, характеризующими штатное их функционирование. Методы статистического анализа имеют различные интерпретации, основанные на различных динамических характеристиках сетевого трафика [1], однако базовые принципы практически у всех идентичны. Неоспоримым преимуществом применения методов статистического анализа является возможность определения впервые реализовываемых методов негативного воздействия на объект атаки со стороны злоумышленника. Однако для его успешной реализации необходимо определить объект анализа, иметь определенные структурированные характеристики, образующие корректную конфигурацию, иметь критерии, по которым можно определить потенциальное протокольное воздействие (ПВ). Для уменьшения вероятности получения ошибочных результатов анализа, основного недостатка применения поведенческих методов выявления инцидентов информационной безопасности, при реализации комплексного подхода, положенного в основу разработки системы протокольной защиты каналов управления роботизированных систем (СПЗ КУ РБС) метод статистического анализа использовался совместно с методами нейросетевого и сигнатурного анализа [2].

Таким образом, основными решаемыми задачами являлись: определение анализируемых и контролируемых характеристик сетевого трафика – признаков ПВ, разработка методик оценки информативности и идентификации признаков ПВ, построение правил штатного функционирования (ПШФ) КУ РБС, разработка алгоритма прогнозирования, а также интеграция методов прогнозирования ПВ в разработанную СПЗ КУ РБС. Для идентификации ПВ необходимо сформировать их сигнатуры. Здесь учитываются как классические признаки ПВ, так и добавочные – фаза ПВ и тип угрозы. Для прогнозирования фиксируется объём данных, т.е. длина пакета.

Таким образом, имеем три признака: "пороговый на основе шаблона штатного функционирования сети (ШШФС)", "доверительного интервала", "доверительного интервала на основе ШШФС". Использование трех признаков сравнения характеристик позволяет с более высокой степенью вероятности выявить именно действия, направленные на нарушение безопасного сетевого взаимодействия. При статистическом анализе необходимо учитывать, что трафик РБС обладает свойством масштабной инвариантности – имеет особую фрактальную (самоподобную) структуру, сохраняющуюся на разных масштабах. В процессе передачи возникают большие всплески при относительно низком среднем уровне трафика, что важно учитывать при статистическом анализе [3].

Производя периодический или постоянный анализ состояния РБС, появляется возможность идентифицировать действия злоумышленников, направленные на подготовку к проведению атак: сканирование портов, службы, получение информации об используемом прикладном, системном программном обеспечении и системах защиты (на этапе рекогносцировки).

Описанные выше методы обнаружения попыток нарушения безопасности в КУ РБС основаны на том обстоятельстве, что в этом случае могут изменяться некоторые статистические характеристики потока пакетов [4]. Сопоставляя результаты, можно сделать вывод, что диапазоны значений характеристик штатного функционирования КУ РБС, имеют относительное постоянство уровней значений математических ожиданий и дисперсий [5]. При возникновении нештатной ситуации аналогичные оценки по различным характеристикам изменяются значительно.

СПИСОК ЛИТЕРАТУРЫ

1. Баранов В.В., Гудков М.А., Крибель А.М., Лаута О.С., Нечепуренко А.П. Защита канала управления роботизированных систем. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 32-37.
2. Елисеев А.И., Долгов А.А., Хорохорин М.А., Лаута О.С., Набатов К.А. Обеспечение живучести информационных систем (часть 3. Методы обеспечения и повышения живучести). Вестник Воронежского института ФСИН России. 2013. №1. С.91-94.

3. Коцыняк М.А., Лаута О.С., Нечепуренко А.П., Штеренберг И.Г. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия. Труды учебных заведений связи. 2016. Т. 2. № 4. С. 82-87.
4. Лепешкин О.М., Карпов А.В., Шостак Р.К. Актуальность осуществления сетевого контроля защищенности информационных сетей. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1198.
5. Баранов В.В., Крибель А.М., Лаута О.С., Нечепуренко А.П. Применение метода топологического преобразования стохастических сетей для оценки эффективности средств защиты. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 47-52.
6. Анисимов В. В. Модель функционирования сети связи общего пользования, учитывающая нагрузку от разнородных абонентов // Санкт-Петербургская международная конференция «Региональная информатика». Сборник трудов. — СПб. : СПИИРАН, 2016. — С. 360—365.

УДК 681.5.391.21

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕТЕЙ СТАНДАРТА IEEE 802.11

Колнооченко Анастасия Александровна
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: kolnoochenko.asya@yandex.ru

Аннотация. Рассмотрены угрозы информационной безопасности, возникающие при использовании беспроводного стандарта.

Ключевые слова: *информационная безопасность; угрозы; беспроводные сети; стандарт IEEE 802.11.*

INFORMATION SECURITY NETWORKS IEEE 802.11

Kolnoochenko Anastasiya
Military Academy of Communications named after SM Budennogo
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: kolnoochenko.asya@yandex.ru

Abstract. Reviewed information security threats arising from the use of a wireless standard.

Keywords: *information security; threats; wireless networks; standard IEEE 802.11.*

В настоящее время широкое распространение получила технология IEEE 802.11, известная как Wi-Fi. Если изначально специальными модулями Wi-Fi комплектовались только носимые компьютеры и мобильные телефоны, то сегодня список данных устройств значительно шире. Возможность поддерживать связь с глобальной сетью есть у львиной доли производимой электроники и техники. Поэтому низкий уровень защиты беспроводных сетей представляет особую опасность[1].

Построение сети стандарта IEEE 802.11 основано на организации точек быстрого доступа и обеспечивает одновременный доступ большого количества абонентов с возможностью перемещения их в области действия сигнала. Появление данной технологии позволило построить сеть там, где нет возможности проложить кабель[2]. Сейчас беспроводные сети используются повсеместно: в общественных местах, крупных и мелких предприятиях. Однако с появлением беспроводных сетей возникли соответствующие угрозы безопасности. Под угрозой информационной безопасности понимается совокупность условий и факторов, создающих потенциальную опасность, связанную с утечкой информации и/или несанкционированным воздействием на нее[3].

Угрозы информационной безопасности, возникающие при использовании беспроводного стандарта, подразделяются на прямы и косвенные. Прямые угрозы возникают непосредственно при передаче данных по сети. К ним относятся, например, блокирование, искажение информации, перехват пакетов, их последующая расшифровка и другие деструктивные воздействия на сеть[4]. Косвенные угрозы информационной безопасности связанны с наличием сетей Wi-Fi вблизи объекта. Они опасны и для информации, обрабатываемой в сети, и для речевой информации. Так, например, причиной утечки важных данных, может стать микрофон мобильного телефона.

Сигналы сети стандарта IEEE 802.11 обладают широким спектром, поэтому обычные устройства радиомониторинга не могут их распознать, точно выявить его можно только вблизи точки доступа. Также скрытию несанкционированной передачи информации способствует наличие по соседству большого числа различных Wi-Fi сетей, так как выявлять нелегальных абонентов необходимо не только среди клиентов одной сети, но и соседних[5].

В технологии Wi-Fi предусмотрены шифрование и аудентификация, но так как их применение в несколько раз уменьшает скорость передачи данных по каналу, данные методы защиты не всегда применяются. Также в некоторых случаях может использоваться устаревшая технология шифрования Wired Equivalent Privacy (WEP), ключи которой можно подобрать, используя специальные программы.

Таким образом, применение технологии Wi-Fi влечет за собой множество угроз информационной безопасности объекта. Способность передавать все виды информации в режиме

реального времени еще больше расширяет возможности перехвата ценной информации. В целях повышения уровня защиты беспроводных сетей стандарта IEEE 802.11 необходимо комплексное использовать аутентификацию (стандарта IEEE 802.1X, аутентификацию по MAC-адресам), шифрование и контроль целостности данных (протокол WPA).

СПИСОК ЛИТЕРАТУРЫ

1. Лихоносов А. Словарь-справочник по информационной безопасности. – М.: МФПА, 2010. С. 390.
2. Олифер В. Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, С. 2010 – 944.
3. WPA2 на защите беспроводных сетей Wi-Fi http://www.technorium.ru/cisco/wireless/wpa2.shtml
4. Лепешкин О.М., Карпов А.В., Шостак Р.К. Актуальность осуществления сетевого контроля защищенности информационных сетей. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1198.
5. К вопросу об оптимизации структуры инфокоммуникационных технологий в автоматизированных системах управления. Лепешкин О.М., Корсунский А.С., Корсунская Д.С. Радиопромышленность. 2011.№ 4. С. 11-17.

УДК 004.056.57

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА КАНАЛА УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ

Коцыняк Михаил Антонович, Гудков Михаил Александрович, Сафонов Алексей Александрович, Борис Артурович Арутюнян
Военная академия связи имени Маршала Советского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: vlasenko199@yandex.ru, asuetin5@yandex.ru

Аннотация. В работе рассмотрен способ защиты канала управления роботизированных систем на основе криптографических алгоритмов.

Ключевые слова: *роботизированная система; канал управления; метод преобразования.*

CRYPTOGRAPHIC PROTECTION OF A CONTROL PATH OF ROBOTIC SYSTEMS

Kocinyak Mikhail, Gudkov Mikhail,Safonov Alexey, Arutunyan Boris
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckystr., 3
e-mail: vlasenko199@yandex.ru, asuetin5@yandex.ru

Abstract. In article, the way of protection of a control path of robotic systems on the basis of cryptographic algorithms is considered.

Keywords: *robotic system; control path; transformation method.*

Автоматизированные и роботизированные системы обладают неразрывной связью между входящими в них вычислительными и физическими элементами. Сегодня представители таких систем могут быть найдены в самых разнообразных областях - космос, автомобильные, химическая технология, гражданская инфраструктура, энергетика, здравоохранение, производство, транспорт, и потребительские устройства. Такой класс систем рассматривается как киберфизические системы [1].

С одной стороны, киберфизические системы за счет распределенной сети датчиков и блоков управления позволяют решить многие практические задачи, позволяющие сэкономить время и уменьшить человеческие потери, за счет выполнения опасных заданий роботизированными системами.

С другой стороны, за счет использования открытых радиоканалов и протоколов киберфизические системы подвержены воздействию компьютерных атак, которые в наилучшем случае могут привести к нарушению работоспособности сети, а в худшем к перехвату управления.

К наиболее распространенным компьютерным атакам на киберфизические системы относятся: активные и пассивные виды компьютерных атак [2].

Учитывая вышеизложенное, в настоящее время остро стоит вопрос о защите киберфизических систем и каналов управления ими. С этой целью предлагается использовать криптографические протоколы и алгоритмы [3].

Для реализации защиты канала управления киберфизической системы, рациональным является симметричный алгоритм AES, который отличается криптостойкостью и быстродействием.

В настоящее время криптография решает следующие основные задачи:

1. Обеспечение конфиденциальности сообщений – решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права к ней.

2. Обеспечение целостности данных – невозможность несанкционированного изменения информации.

3. Аутентификация – подтверждение подлинности сторон и самой информации в процессе обмена данными.

4. Невозможность отказа от авторства – предотвращение отказа от совершенных действий.

Эти задачи защиты данных реализованы в специальном аппаратном блоке, который называют криптографическим ускорителем (криптографическим блоком).

Для обеспечения криптографически стойкого протокола управления в разработанной роботизированной системе используется микроконтроллер с 32-разрядным ядром ARM Cortex–M4F с криптографическим ускорителем stm32f415rgt производства компании «STMicroelectronics». Для того, чтобы чип дешифровал принятые пакеты, в качестве алгоритма дешифрования используется AES с длиной ключа 128 бит.

В качестве алгоритма распределения ключей был рассмотрен и реализован алгоритм Диффи–Хеллмана [4], который позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищенный от подмены, канал связи.

Таким образом, представлен наглядный пример создания роботизированного комплекса, как элемента КБС[5], с защищенной системой управления на основе алгоритма шифрования AES, являющимся на сегодняшний момент наиболее криптостойким.

Кроме того, для защиты от атаки «грубого перебора» криптографического ключа в системе управления необходимо реализовывать алгоритм распределения ключей, позволяющий генерировать новый ключ, каждый раз перед выполнением команды.

СПИСОК ЛИТЕРАТУРЫ

1. Елисеев А.И., Долгов А.А., Хорохорин М.А., Лаута О.С., Набатов К.А. Обеспечение живучести информационных систем (часть 3. Методы обеспечения и повышения живучести). Вестник Воронежского института ФСИН России. 2013. №1. С.91-94.
2. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П.Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 83-89.
3. Баранов В.В., Гудков М.А., Крибель А.М., Лаута О.С., Нечепуренко А.П. Защита канала управления роботизированных систем. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 32-37.
4. Коцыняк М.А., Карганов В.В., Лаута О.С., Нечепуренко А.П. Методика обоснования мер противодействия радиолокационной разведке высокоточного оружия. Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. № 9-10 (99-100). С. 54-57.
5. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. Модель таргетированной кибернетической атаки. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 90-98.
6. Стародубцев Ю.И., Бречко А.А., Львова Н.В. Необходимость оценки защищенности системы связи от средств информационной борьбы в современных условиях. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1201.

УДК 004.056.57

МЕТОДИКА ПРОГНОЗИРОВАНИЯ ВОЗДЕЙСТВИЯ ТАРГЕТИРОВАННОЙ КИБЕРНЕТИЧЕСКОЙ АТАКИ НА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННУЮ СЕТЬ

Коцыняк Михаил Антонович, Иванов Денис Александрович, Лаута Олег Сергеевич,
Нечепуренко Александр Петрович, Муртазин Ильдар Робертович
Военная академия связи имени Маршала Советского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: prosto_deniss@mail.ru

Аннотация. Рассматривается логико-вероятностный метод оценки опасности таргетированной кибернетической атаки, позволяющий выбрать вариант защиты элементов информационно-телекоммуникационной сети.

Ключевые слова: *таргетированная кибернетическая атака; анализ иерархий; информационно-телекоммуникационная сеть.*

METHOD OF PREDICTING THE IMPACT OF A TARGETED CYBERNETIC ATTACK ON THE INFORMATION AND TELECOMMUNICATIONS NETWORK

Kociniak Mihail, Ivanov Denis, Lauta Oleg, Nechepurenko Aleksandr, Murtazin Ildar
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckystr., 3
e-mail: prosto_deniss@mail.ru

Abstract. In the article the logical-probabilistic method for assessing the danger of a target cybernetic attack is considered, which makes it possible to chose the protection option for information and telecommunications network.

Keywords: *target cybernetic attack; analysis of hierarchies; information and telecommunications network.*

Основной тенденцией последних лет является смещение акцента с массовых атак на таргетированные, или целевые, которые заранее планируют действия противника. Целевая атака всегда строится под объект воздействия, являясь продуманной операцией, а не простым техническим действием. Высокая сложность их обнаружения и колоссальный урон от их действий, который не гарантированно может быть обнаружен спустя длительный срок. Таргетированная (целевая) кибернетическая атака (ТКА) на элементы информационно-телекоммуникационной сети (ИТКС) реализуется в виде проведения комплекса мероприятий по изучению информационной системы и программного обеспечения [1].

При воздействии ТКА на ИТКС затруднительно выбрать способы и средства защиты, так как ресурс ограничен. Одним из путей разрешения является дифференцированный подход к защите ИТКС и ее элементов, который заключается в выборе наиболее актуальных для сложившейся обстановки направлений защиты. Для обоснования направлений защиты ИТКС и ее элементов, ассиметричных возможностям ТКА, необходимо разработать методику прогнозирования воздействия ТКА противником на ИТКС и ее элементы. В настоящее время отсутствуют методики, предназначенные для этого. С целью прогнозирования предлагается методика прогнозирования воздействия ТКА на ИТКС.

Целью методики является прогнозирование ТКА с учётом места и роли элементов в ИТКС, определение очерёдности воздействия на элементы ИТКС и наиболее опасных ТКА, что, в свою очередь, позволит формировать исходные данные для принятия мер защиты элементов и ИТКС в целом.

Методика предназначена для обоснования принятия решений по защите элементов ИТКС от ТКА должностными лицами на этапах формирования, развёртывания и функционирования ИТКС ОЗУ.

Результатом прогнозирования воздействия ТКА на ИТКС будет матрица назначений ТКА противника на элементы ИТКС, а также очерёдность воздействия на них.

В основу методики положено определение степени опасности ТКА, для чего необходимо рассмотреть физические основы этапов ТКА, особенности их воздействия, характер проявления на элементах ИТКС.

Оценка опасности ТКА на ИТКС вызывает некоторое затруднение, связанное с недостаточной разработкой соответствующего методического аппарата. Для оценки опасности ТКА предлагается использовать логико-вероятностные методы [2].

Одним из наиболее распространённых логико-вероятностных методов является метод анализа иерархий, который позволяет понятным и рациональным образом структурировать сложную проблему принятия решений в виде иерархии, сравнить и выполнить количественную оценку альтернативных вариантов решения. Поэтому для оценки опасности ТКА для ИТКС предлагается использовать метод анализа иерархий [3].

За степень опасности ТКА относительно вскрытия элементов ИТКС примем:

- степень воздействия на линию связи;
- степень воздействия на маршрутизатор;
- степень воздействия на коммутатор;
- степень воздействия на персональные электронно-вычислительные машины;
- степень воздействия на сервер электронной почты;
- степень воздействия на сервер базы данных;
- степень воздействия на сервер web.

На основании результатов учитывая идею распределения разноэффективных этапов ТКА по взаимозависимым, с различной степенью важности, элементам ИТКС, виды целевой функции и ограничений, в условия решения задачи, приемлемым методом решения является метод двух функций. Таким образом, разработана методика оценки комплексного информационного воздействия на основе распределения разнородного ресурса по взаимоувязанным элементам ИТКС, которая позволяет определить угрозы ИТКС и обосновать асимметричные им меры защиты. Данный метод позволяет оценить угрозы для элементов ИТКС по уровням ЭМВОС и на каждом уровне формировать постановку задачи на синтез системы защиты ИТКС в условия воздействия ТКА [4].

Заключение. Анализ полученных результатов показал, что в первую очередь ТКА будут направлены на линию связи и маршрутизатор, а наиболее часто используемой является ТКА типа «Сканирование сети и ее уязвимостей». Полученные результаты позволяют обосновать дифференцированный подход при выборе варианта защиты элементов ИТКС.

Необходимо отметить, что рассматриваемую задачу, исходя из характера действий ИТКС и принципов планирования, нужно решать для временных «сечений» по этапам функционирования системы управления.

В этом случае после каждой смены этапа функционирования необходимо производить уточнение структуры и варианта защиты элементов ИТКС.

СПИСОК ЛИТЕРАТУРЫ

1. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 83-89.
2. Модель таргетированной кибернетической атаки. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 90-98.
3. Стародубцев Ю.И., Бречко А.А., Львова Н.В. Необходимость оценки защищенности системы связи от средств информационной борьбы в современных условиях. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1201.
4. Защита канала управления роботизированных систем. Баранов В.В., Гудков М.А., Крибель А.М., Лаута О.С., Нечепуренко А.П. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 32-37.
5. Кулешов И.А., Расчесова А.Г., Львова Н.В. Оценка эффективности системы связи по комплексному показателю. // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2009. Т. 1. № 72. С. 33-37.
6. Стародубцев Ю.И., Бречко А.А., Львова Н.В. Необходимость оценки защищенности системы связи от средств информационной борьбы в современных условиях. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1201.

УДК004.056

ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Киреев Сергей Хаирбекович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: gamlet8806@rambler.ru

Аннотация. В докладе описан подход к обнаружению сетевых аномалий, образованных в результате проведения таргетированных компьютерных атак на информационно-телекоммуникационные сети, основанный на проведении анализа сетевой активности и выделения признаков аномального поведения с использованием методов машинного обучения и искусственного интеллекта. В качестве математического аппарата для реализации предлагаемого подхода рассматриваются искусственные нейронные сети, позволяющие решать задачи классификации и прогнозирования, и рассматриваются возможные варианты применения искусственных нейронных сетей для обнаружения аномального поведения в информационно-вычислительной сети.

Ключевые слова: *информационно-вычислительная сеть; компьютерные атаки; системы обнаружения атак; искусственный интеллект; машинное обучение; нейронные сети; репликатор нейронной сети; таргетированная атака; APT-угрозы.*

APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS IN TASKS OF INFORMATION SECURITY SUPPORT

Kireev Sergey
The S.M. Budjonny Military Academy of the Signal Corps
Russia, St. Petersburg, Prospect Tikhoretsky, 3
e-mail: gamlet8806@rambler.ru

Abstract. The report describes an approach to detect network anomalies formed as a result of targeted computer attacks on information and telecommunication networks based on the analysis of network activity and the isolation of signs of abnormal behavior using machine learning techniques and artificial intelligence. As a mathematical apparatus for the implementation of the proposed approach, artificial neural networks that solve classification and prediction problems are considered, and possible applications of artificial neural networks for detecting abnormal behavior in the information network are considered.

Keywords: *information-computer network; computer attacks; intrusion detection systems; artificial intelligence; machine learning; neural networks; neural network replicator; targeted attack; APT-threats.*

Подходы к построению систем обеспечения информационной безопасности.

5 декабря 2016 года Президент России Владимир Путин подписал Указ об утверждении новой Доктрины информационной безопасности Российской Федерации. Новый документ пришел на смену Доктрине, утвержденной 9 сентября 2000 года, которая признается утратившей силу. Но далеко не все реализуемые специалистами по информационной безопасности на протяжении этого срока меры можно признать успешными [1].

Киберугрозы представляют собой постоянную опасность не только для военной индустрии, но и мировой экономики в целом [2]. По прогнозам, в течение следующего года киберугрозы превысят

отметку в триллион долларов, если говорить о размере причиненного ущерба. Для уменьшения приливной волны киберпреступности, захлестнувшей Россию, Европу, США и, в определенной степени, весь остальной мир, требуется сделать намного больше.

Традиционные решения большинства антивирусных компаний, лишь ограничиваются осуществлением контроля доступа к информационным ресурсам и их мониторингом. Такой подход позволяет хорошо справляться с известными вирусами или вредоносными программами, но почти бессилен против широко распространенных в последнее время таргетированных угроз (APT-угроз).

Стандартная APT-угроза включает в себя использование хакером уязвимости «нулевого дня» и установку кейлоггера. Воспользовавшись похищенными учетными записями, хакер получает доступ в IT-системы и имеет возможность скачать конфиденциальную корпоративную информацию. Даже SIEM-системы не способны обеспечить полную защиту от угроз уязвимости «нулевого дня», следовательно, этот вид атаки становится практически не распознаваемым, а шансы предотвратить его — крайне низкими. Всё это послужило причиной к тому, что компании из сферы IT-безопасности уже начали разрабатывать и применять свои собственные решения, связанные с анализом поведения пользователей [3-5].

Благодаря этому, машинное обучение вскоре станет новой нормой, наравне с информационной безопасностью, управлением событиями или SIEM, и, в конечном итоге, в течение ближайших пяти лет вытеснит большую часть традиционных антивирусов, эвристики и других систем основанных на анализе сигнатур.

APT-угрозы.

Таргетированная атака (APT-угроза) заключается в непрерывной несанкционированной активности в инфраструктуре атакуемой системы, удаленно управляемый в реальном времени вручную. Данный процесс направлен на конкретные инфраструктуры, призван преодолеть конкретные механизмы безопасности, определенные продукты, вовлечь во взаимодействие конкретных сотрудников.

Таргетированная атака имеет следующий жизненный цикл:

1. Подготовка. Основная задача первой фазы — найти цель, собрать о ней достаточно детальной приватной информации, опираясь на которую выявить слабые места в инфраструктуре. Выстроить стратегию атаки, подобрать ранее созданные инструменты, доступные на черном рынке, либо разработать необходимые самостоятельно. Обычно планируемые шаги проникновения будут тщательно протестированы, в том числе на необнаружение стандартными средствами защиты информации.

2. Проникновение — активная фаза целевой атаки, использующая различные техники социальной инженерии и уязвимостей нулевого дня, для первичного инфицирования цели и проведения внутренней разведки. По окончании разведки и после определения принадлежности инфицированного хоста (сервер/рабочая станция) по команде злоумышленника через центр управления может загружаться дополнительный вредоносный код.

3. Распространение — фаза закрепления внутри инфраструктуры преимущественно на ключевые машины жертвы. Максимально распространяя свой контроль, при необходимости корректируя версии вредоносного кода через центры управления.

4. Достижение цели — ключевая фаза целевой атаки.

Наиболее успешным методом противодействия таргетированным атакам является мониторинг и своевременное выявление запущенных неконтролируемых процессов в информационно-телекоммуникационной сети. Можно выделить два основных класса мер — хорошо знакомый всем набор технических решений, способных прервать сетевую коммуникацию или запуск какого-то процесса в инфраструктуре, и машинное обучение (обучение с помощью искусственного интеллекта).

Становится понятно, что ИНС позволяют эффективно решать задачи, связанные с обнаружением аномального поведения в процессе управления функционирования и информационного обмена в ИВС. Таким образом, использование ИНС позволит повысить защищённость ИВС и обеспечить более высокий уровень обнаружения КА по сравнению с традиционно-используемыми средствами защиты, так как в отличие от сигнатурных СОА способны к обобщению имеющихся знаний и использованию их для обнаружения новых типов КА.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ;
2. Хайкин С. Нейронные сети: полный курс, 2-е издание: Пер. с англ. – М.: Издательский дом «Вильямс», 2006.
3. Горбань А. Н., Дунин-Барковский В. Л. и др. Нейроинформатика. — Новосибирск: Наука, 1998;
4. Еремин Д. М., Гарцеев И. Б. Искусственные нейронные сети в интеллектуальных системах управления. — М.: МИРЭА, 2004. — 75 с. — ISBN 5-7339-0423-2;
5. Ясницкий Л. Н. Введение в искусственный интеллект. — М.: Издат. центр «Академия», 2005. — 176 с. — ISBN 5-7695-1958-4.

УДК 681.5.015

ПРОБЛЕМА ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОГО СОПРЯЖЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ РАЗЛИЧНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Кондрашов Юрий Владимирович, Максименко Евгений Алексеевич
Военная академия связи имени Маршала Советского Союза С. М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail:dima7.borets@mail.ru

Аннотация. Сформулированы общие проблемы по организационно-техническому сопряжению систем защиты информации в различных автоматизированных системах управления специального назначения, а также предпринята попытка предъявить единые требования, предъявляемые к ним.

Ключевые слова: *система защиты информации; автоматизированная система управления специального назначения; проблемы сопряжения.*

THE PROBLEM OF ORGANIZATION TECHNICAL COUPLING SYSTEM OF PROTECTION OF INFORMATION OF VARIOUS AUTOMATED CONTROL SYSTEM OF SPECIAL PURPOSE

Kondrashov Yuri, Maksimenko Yevgeniy
Millitary Academy of Communications named S.M. Budyonnogo.
Russia, St. Peterburg, Tikhoretsky pr., 3
e-mail:dima7.borets@mail.ru

Abstract. General problems on the organizational and technical interface of information security systems in various automated control systems for special purposes have been formulated, and an attempt has been made to present uniform requirements for them.

Keywords: *Information security system; automated control system for special purposes; coupling problems.*

Особенностями современной автоматизированной системы управления специального назначения (АСУ СН) является модульное построение ее элементов, стандартизация и унификация аппаратных и программных средств. Функционирование такой АСУ СН возможно при соединении необходимыми вертикальными и горизонтальными связями всех звеньев управления и взаимодействия между собой, что позволяет расширить информационное пространство контура управления. Результатом объединения должна стать многоуровневая иерархия АСУ СН. В каждой из них могут быть выделены управляющая и управляемые АСУ СН, вертикальные стволы управления и горизонтальные связи взаимодействия. Обмен информацией в сетях управления АСУ СН должны обеспечить комплексы средств автоматизации специального назначения (КСА), а также комплексы средств телекоммуникаций, связи и обмена данными реального времени (строящихся на сетевых принципах), как межвидовые открытые системы, позволяющие наращивать количество потребителей независимо от их уровня управления, места размещения и выполняемых задач в пределах своей максимальной производительности [1].

Однако, в настоящее время в АСУ СН разных уровней управления остаются КСА разработанные на разных заводах изготовителях, изготовленные по разным технологиям, не увязанные единым замыслом по вопросам информационной, лингвистической, программной и технической совместимости.

Кроме этого отсутствуют единые технологии и стандарты, позволяющие всем предприятиям, участвующим в процессе, действовать в общем методологическом и технологическом пространстве, что, естественно, особенно отрицательно сказывается при осуществлении крупных проектов.

А широкая номенклатура систем защиты информации (СЗИ), используемых в большинстве КСА и АСУ СН, как правило создается, с использованием только программных средств (без средств криптозащиты).Таким образом, наличие множества различных СЗИ делает невозможным создание единой (сквозной) системы защиты сложных АСУ СН, существенно усложняет комплексирование различных КСА в АСУ СН, приводит к разного рода нарушениям порядка доступа к информации.

Все вышеперечисленное приводит к несовместимости существующих и создаваемых КСА различных АСУ СН, к снижению эффективности их применения, дублированию и удорожанию разработок, невозможности эффективного функционирования информационно-управляющих систем АСУ СН. Наличие многочисленных протоколов взаимодействия приводит к не стыковке различных КСА и их СЗИ между собой и, как следствие, к необходимости разработки соответствующих шлюзов, снижающих скорость обмена информацией, невозможности работы через современные системы обмена данными между КСА различных АСУ СН [2].

Для решения проблемы неунифицированных СЗИ целесообразно обеспечить единый подход к созданию систем защиты информации для всех КСА и АСУ СН [3] (единые криптографические принципы СЗИ от несанкционированного доступа (НСД), работа с информацией, имеющей различные

степени безопасности, взаимодействие различных КСА и АСУ СН с точки зрения СЗИ от НСД, защита баз данных и т.д.).

В соответствии с вышеперечисленным возникают проблемы организационно-технического сопряжения СЗИ КСА различных АСУ СН, которые могут быть разрешены путем разработки предложений по единым требованиям, предъявляемым в тактико-технических заданиях к ним, увязанных единым замыслом по вопросам информационной, лингвистической, программой и технической совместимости.

СПИСОК ЛИТЕРАТУРЫ

1. Анфилатов В.С., Авраменко В.С., Пантюхин О.И. Теоретические основы автоматизации управления войсками и связью. Часть 2. Основы построения и функционирования систем автоматизации управления войсками и связью: Учеб. пособие. – СПб.: ВАС, 2015г. – 304с.
2. Ионов С.В. К вопросу обеспечения совместимости в автоматизированных системах управления. Информационные технологии №1. Системы, средства связи и управления: Информационно-аналитический сборник / Под ред. С.В. Ионова; АО «Концерн «Созвездие». Воронеж, 2012. № 2. 166 с.: ил.
3. Бирюков М.А. Разработка модели нарушителя правил разграничения доступа к единому информационному пространству // Математические методы в технике и технологиях – ММТТ. 2017. Т.3. С. 107-110.

УДК 004.056.53

МЕТОДИКА ОЦЕНКИ КОМПЛЕКСНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ИТКС СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Коцыняк Михаил Антонович, Ястребов Владимир Васильевич,
Клиншов Илья Андреевич, Гулевич Антон Владимирович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: dmitry-chikov@rambler.ru

Аннотация. В докладе рассмотрена методика прогнозирования распределения КА с учетом места и роли элементов в ИТКС, определение очередности воздействия на элементы ИТКС и наиболее опасных КА, что в свою очередь, позволит формировать исходные данные для принятия мер защиты элементов и ИТКС в целом.

Ключевые слова: *матрица; дифференцированный; субэлементы.*

SSESSMENT METHODOLOGY OF INTEGRATED INFORMATION IMPACT OF INFORMATION AND TELECOMMUNICATION SYSTEMS SPECIAL PURPOSE

Kocinac Michael, Yastrebov Vladimir, Klinshov Ilya, Gulevich Anton
Military Academy of communications
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: dmitry-chikov@rambler.ru

Abstract. The article considers the methodology of forecasting the distribution of KA taking into account the place and role of elements in information and telecommunication systems, prioritizing the impact on the elements of ITKs and the most threat ON, which in turn, will generate baseline data for the adoption of measures of protection elements and of ITKs in General.

Keywords: *matrix; different; sub.*

Анализ построения современных ИТКС показывает, что их архитектурные решения в общем случае идентичны. Они представляют собой территориально распределённые системы, объединяющие в своем составе ЛВС и отдельные компьютеры, которые осуществляют обмен данными друг с другом и могут иметь общие ресурсы и единое управление.

Увеличение объёмов хранимой и передаваемой информации, территориальная распределенность сетей связи приводит к наращиванию потенциальных возможностей для технической компьютерной разведки противника.

Основным воздействующим фактором на ИТКС являются компьютерные атаки (КА), являющиеся частью информационного воздействия.

Очевидно, что в условиях информационного воздействия (ИВ) довольно затруднено выбрать средства и способы защиты ИТКС, так как ресурс ограничен. Одним из путей разрешения этого противоречия является дифференцированный подход к защите ИТКС и ее элементов, который заключается в выборе наиболее актуальных для сложившейся обстановки направлений защиты. Для обоснования направления защиты и ее элементов, ассиметричных возможностям КА, необходимо разработать методику оценки воздействия КА на ИТКС и ее элементы.

Целью методики является прогнозирование распределения КА с учетом места и роли элементов в ИТКС, определение очередности воздействия на элементы ИТКС и наиболее опасных КА, что в свою очередь, позволит формировать данные для принятия мер защиты элементов и ИТКС.

В основу методики положено определение степени опасности КА, для чего необходимо рассмотреть физические основы отдельных КА, особенности их воздействия, характер проявления на элементах ИТКС.

Методика предназначена для обоснования принятия решений по защите элементов ИТКС от КА должностными лицами на этапах формирования, развертывания и функционирования ИТКС.

Результатом оценки ИВ на ИТКС является матрица сравнения критериев опасности КА на элементы ИТКС. Матрица сравнения критериев опасности КА, выражающий весовые значения критериев относительно общей цели (вскрытие ИТКС). Таким образом, используя метод анализа иерархий, представляется возможным определить вероятность воздействия на субэлементы ИТКС оцениваемыми КА. Полученные результаты могут быть уточнены на этапе детального планирования при аналитической защищенности ИТКС.

СПИСОК ЛИТЕРАТУРЫ

1. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия. Радиолокация, навигация, связь.Международная научно-техническая конференция. В 3-х томах. 2017. С. 83-89
2. Лепешкин О.М., Харечкин П.В., Анализ Моделей Разграничения Доступа, Реализованных В Современных Социотехнических Системах. Инфокоммуникационные технологии. 2008. Т. 6. № 2. С. 91-93.
3. Антонюк Л.Я., Игнатов В.В. Эффективность радиосвязи и методы её оценки. – СПб.: ВАС, 1994. – 138 с.
4. Лепешкин О.М. Исследование Функциональной Безопасности Систем Государственного Управления. Инфокоммуникационные технологии. 2007. Т. 5. № 3. С. 165-166.
5. Куприянов А.И., Шустов Л.Н. Радиоэлектронная борьба. Основы теории., 2011. – 789 с.

УДК 004.056

ЗАЩИТА ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННЫМ КАНАЛАМ СВЯЗИ ПОЧТОВЫХ СЕРВЕРОВ

Крибель Александр Михайлович, Корякин Денис Дмитриевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: mrl.may.hacking@gmail.com

Аннотация. В работе описан подход к обеспечению безопасности информации, передаваемой по информационно телекоммуникационным каналам связи почтовых серверов военного назначения, основанный на криптографической защите библиотеки PGP. Данный подход применим, прежде всего, в военной сфере и является актуальным на сегодняшний день.

Ключевые слова: *криптостойкость; PGP; сессионный ключ; криптоанализ; информационная безопасность.*

INFORMATION SECURITY, TRANSFERRED ON INFORMATION AND TELECOMMUNICATION CHANNELS OF MAIL SERVERS

Kribel Alexander, Denis Koryakin
S.M. Budjonny Military Academy of the Signal Corps
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: mrl.may.hacking@gmail.com

Abstract. This paper describes the approach to ensuring information security of mail servers for military purposes transmitted via information telecommunications channels, based on the cryptographic protection of the PGP library. This approach is applicable, first of all, in Military sphere and is relevant for today.

Keywords: *cryptostabilityi; PGP;one-time key; cryptanalysis; information security.*

В результате борьбы с терроризмом во многих странах, в том числе и в Российской Федерации, были приняты законы, которые обязывают интернет-провайдеров архивировать всю переписку своих клиентов. Спецслужбы крупных государств регулярно сканируют электронную почту в поиске подозрительных ключевых слов и фраз. Вот лишь несколько таких государственных программ: международная система ECHELON (США), проект Carnivore (США), системы СОРМ и СОРМ-2 (Россия). Однако научно-технический прогресс не только облегчил задачу слежения за электронной перепиской, но этот же прогресс позволяет переписку надежно защитить, от противоборствующих стран и террористических организаций, стремящихся получить доступ к информации.

Мощнейшим оружием в борьбе за информационную безопасность являются криптографические методы защиты информации. Одним из самых надёжных криптографических решений для шифрования электронной почты с открытым ключом является протокол сети доверия — PGP.

Когда Эдвард Сноуден говорил «шифрование работает», он подразумевал именно протокол PGP. Данный протокол позволяет выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде, в том числе прозрачное

шифрование данных на запоминающих устройствах, например, на жёстком диске [1]. Устойчивость PGP базируется на фундаментальных нерешенных математических задачах.

Создатель первой программы PGP, Филипп Циммерман, открыто опубликовал ее код в 1991 году. Вскоре после выпуска PGP стала использоваться за пределами США, и в 1993 году правительство США начало расследование против Циммермана по подозрению в нарушении экспортного законодательства, которое регулирует распространение криптографических систем с длиной ключа более 40 бит. В PGP использовались ключи длиной 128 бит и более.

Циммерман обошёл ограничения законодательства США, опубликовав исходный код в книге, изданной MIT Press[2, 3]. Код можно было отсканировать, распознать и скомпилировать. Экспорт книг не может быть запрещён, так как защищён первой поправкой к Конституции США.

В 1996 году расследование было закрыто [4][5].

С тех пор программу неоднократно исследовали криптоаналитики высочайшего класса и ни один из них не нашел в используемых методах шифрования слабых мест.

Шифрование PGP построено на принципе несимметричной криптографии и решает три задачи конфиденциального обмена информацией:

1. Защищает текст сообщений от посторонних. То есть прочитать сообщение может только человек, у которого есть секретный ключ и который знает пароль.
2. Подтверждает получателю целостность приходящего сообщения. То есть дает уверенность в том, что при передаче содержание сообщения не изменилось.
3. Подтверждает личность отправителя. Встроенная в PGP электронная подпись однозначно идентифицирует отправителя, поскольку только он имеет доступ к секретному ключу и знает пароль.

Прежде чем зашифровать сообщение отправитель определяет получателя. PGP находит публичный ключ получателя (для этого он должен быть в файле публичных ключей на компьютере отправителя).

Перед шифрованием PGP сжимает текст сообщения. Это ускоряет передачу и увеличивает надежность шифрования. Затем генерируется так называемый сессионный (одноразовый) ключ, который представляет собой длинное случайное число. С помощью сессионного ключа шифруется текст сообщения. Текст сообщения шифруется с помощью алгоритма симметричного шифрования. В этом алгоритме для шифрования и дешифрования используется один ключ. Поэтому для дешифрования сообщения получатель тоже должен иметь этот сессионный ключ. Однако отправлять этот ключ в открытом виде небезопасно, поэтому он шифруется публичным ключом получателя. Зашифрованный сессионный ключ отправляется получателю вместе с зашифрованным текстом. Необходимость использовать симметричный алгоритм шифрования обусловлена его высокой скоростью.

Расшифровка сообщений происходит в обратной последовательности. На компьютере получателя PGP использует его секретный ключ для расшифровки сессионного ключа. С помощью этого ключа дешифруется текст сообщения.

В 1996 году криптограф Брюс Шнайер охарактеризовал раннюю версию PGP как «ближайшую к криптосистемам военного уровня». На данный момент не известно ни одного способа взлома данных, зашифрованных PGP, при помощи полного перебора или уязвимости криптоалгоритма.

Криптографическая стойкость PGP основана на предположении, что используемые алгоритмы устойчивы к криптоанализу на современном оборудовании

Заключение. Становится понятно, что PGP позволяет эффективно решать задачи, связанные с защитой информации, передаваемой по информационно телекоммуникационным каналам связи почтовых серверов военного назначения. Таким образом, использование данного протокола позволяет подтвердить личность отправителя, целостность сообщения, а также защитить текст сообщения от посторонних. На сегодняшний день данный протокол не является стандартизованным в Российской Федерации, однако прямых законодательных запретов на его использование нет. Законодательно ограничивается использование криптографии только в государственных и муниципальных учреждениях. ФСБ предписывает всем государственным структурам использовать только сертифицированные средства криптографии. Физические лица и компании сами устанавливают, какая информация является для них коммерческой тайной, методы хранения и передачи такой информации [6]. Также авторы проекта «openPGP в России» утверждают, что не существует законов, запрещающих использование PGP [7]. Электронная подпись, генерируемая с помощью PGP и её несертифицированных аналогов, имеет юридическую силу в Российской Федерации, так как согласно пункту 3 статьи 5 63-ФЗ «Об электронной подписи» [8] попадает под определение усиленной неквалифицированной электронной подписи. Согласно пункту 2 статьи 6 этого ФЗ для признания такой ЭП необходимо соглашение между участниками электронного взаимодействия.

СПИСОК ЛИТЕРАТУРЫ

1. Свободная энциклопедия Википедия, статья "PGP" URL: https://ru.wikipedia.org/wiki/PGP (дата обращения: 26.08.2017);
2. Zimmermann, Philip (1995). PGP Source Code and Internals. MIT Press. ISBN 0-262-24039-4;
3. Declaration of Robert v. Prior, OCTOBER 4, 1996 - Показания издателя по делу Bernstein v. US Department of Justice;

4. Feds Won't Prosecute PGP Creator, January 11, 1996, Phil Zimmermann;
5. Here's the announcement from my lead defense counsel / Phil Zimmermann, 1996-01-12;
6. ФЗ «О коммерческой тайне» № 98-ФЗ Статья 10 «Охрана конфиденциальности информации»;
7. OpenPGP в России / Часто задаваемые вопросы / openPGP в России URL: https://www.pgpru.com;
8. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ;

УДК 004.056.57

ВЕРОЯТНОСТНО-ВРЕМЕННЫЕ ХАРАКТЕРИСТИКИ АТАК НА РОБОТИЗИРОВАННЫЕ СИСТЕМЫ

Кузнецов Сергей Иванович, Иванов Денис Александрович, Власенко Максим Андреевич,
Латушко Николай Александрович
Военная академия связи имени МаршалаСоветского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: vlasenko199@yandex.ru, asuetin5@yandex.ru

Аннотация. В работе рассматриваются атаки на роботизированные системы, а также представлен подход к определению их вероятностно – временных характеристик.

Ключевые слова: *роботизированная система; таргетированная кибернетическая атака; метод преобразования.*

PROBABILISTIC AND TIME CHARACTERISTICS OF THE ATTACKS TO ROBOTIC SYSTEMS

Kuznetsov Sergey, Ivanov Denis, Vlasenko Maxim, Latushko Nikolay
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckystr., 3
e-mail: vlasenko199@yandex.ru, asuetin5@yandex.ru

Abstract. In article, the attacks to robotic systems are considered, and approach to definition of their probabilistic and time characteristics is also presented.

Keywords: *robotic system; targeted cybernetic attack; transformation method.*

XXI Век - век информационных технологий, в котором все очень быстро меняется. В настоящее время мир стоит на грани новой промышленной революции – четвертой или Индустрия 4. «Умные» фабрики, заводы-принтеры и интернет вещей уже заменяют человека в производстве.

Основные компоненты Индустрии 4.0: умные сенсоры, которые позволяют собирать данные в процессе производства; передача больших объёмов данных людям, другим машинам и заводам; облачные сервисы, которые предоставляют данные из любого места; «умные станки», которые сами определяют свою производственную траектории, т.е. охватывают все сферы жизни человека.

Технологически это означает не только создание «единой сети станков и машин», но и самостоятельную и непрерывную оптимизацию их текущей работы, большую гибкость производств, персонализацию заказов и более тесную связь с потребителем.

В рамках проекта немецкого правительства Industry 4.0 по компьютеризации промышленности в 2006 году Хелен Джилл ввел понятие киберфизические системы, которые включают в себя:

- системы управления производством;
- беспилотные летательные аппараты и автомобили;
- системы военного назначения;
- роботизированные системы.

Особое внимание зарубежное руководство уделяет внимание роботизированным системам. В качестве основных каналов воздействия на них рассматривают следующие:

- воздействия на подсистемы управления;
- воздействие на человеко-машинный интерфейс;
- воздействия на протоколы взаимодействия;
- воздействия на устройства, входящие в роботизированные системы.

С целью воздействия на роботизированные системы злоумышленник перешел от массовых атак к таргетированным, или целевым. Целевая атака всегда строится под объект воздействия, являясь продуманной операцией. Отличием от других атак является: адресность; скрытность; продолжительность; использование разнородных инструментов и методов; изменчивость вектора атаки, ее инструментария по мере развития; наличие центра управления атакой; результативность.

Таргетированная кибернетическая атака (ТКА) [1] обладает вероятностно-временными характеристиками (ВВХ), определение их позволит оценить степень их опасности, выбрать и реализовать меры защиты. С этой целью предлагается использовать профильные модели ТКА и метод топологического преобразования стохастических сетей (ТПСС) [2].

Профильная модель – условное представление (последовательность действий или алгоритм) реального объекта, системы или процесса (компьютерных атак) в форме, которая создается для более глубокого изучения их функционирования [3].

Стохастическая сеть – совокупность взаимоувязанных узлов (вершин) и ветвей, соединение которых соответствует алгоритму функционирования исследуемой системы [4].

В методе ТПСС исследуется не система, а целевой процесс, который она реализует. Этот сложный процесс декомпозируется на элементарные, каждый из которых может характеризоваться функцией распределения времени его выполнения, плотностью вероятности, вероятностью или средним и дисперсией времени выполнения.

Сущность метода ТПСС состоит в представлении анализируемого процесса в виде стохастической сети, замене множества элементарных ветвей сети одной эквивалентной и последующим определением эквивалентной функции сети, начальных моментов и функции распределения случайного времени ее реализации [5], т.е. реализации анализируемого процесса.

Анализ вероятностно-временных характеристик ТКА позволит обосновать направления разработки системы защиты РТС, целью которой является предотвращение (затруднение) реализации ТКА.

СПИСОК ЛИТЕРАТУРЫ

7. Коцыняк М.А., ИвановА., Лаута О.С., Нечепуренко А.П. Модель таргетированной кибернетической атаки. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 90-98.
8. Баранов В.В., Крибель А.М., Лаута О.С., Нечепуренко А.П.Применение метода топологического преобразования стохастических сетей для оценки эффективности средств защиты. В сборнике: Актуальные проблемы обеспечения информационной безопасности. Труды Межвузовской научно-практической конференции. 2017. С. 47-52.
9. Коцыняк М.А., Карганов В.В., Лаута О.С., Нечепуренко А.П. Методика обоснования мер противодействия радиолокационной разведке высокоточного оружия. Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. № 9-10 (99-100). С. 54-57.
10. Баранов В.В., Гудков М.А., Крибель А.М., Лаута О.С., Нечепуренко А.П. Защита канала управления роботизированных систем. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 32-37.
11. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 83-89.
12. Кулешов И.А., Расчесова А.Г., Львова Н.В. Оценка эффективности системы связи по комплексному показателю. // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2009. Т. 1. № 72. С. 33-37.

УДК 004.056.53

УСТОЙЧИВОСТЬ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ В УСЛОВИЯХ КОМПЬЮТЕРНЫХ АТАК

Кузнецов Сергей Иванович, Новиков Павел Аркадьевич, Кузнецова Анастасия Алексеевна
Военная академия связи имени МаршалаСоветского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: Novikov.p.ark@yandex.ru

Аннотация. В докладе рассматривается киберустойчивость, как составляющая устойчивости информационно-телекоммуникационной сети от компьютерных атак, а также решение проблемы обеспечения киберустойчивости.

Ключевые слова: *компьютерная атака; киберустойчивость; противник; информационно-телекоммуникационная сеть.*

THE STABILITY OF THE INFORMATION AND TELECOMMUNICATIONS NETWORK IN THE CONDITIONS OF COMPUTER ATTAKS

Kuznesov Sergey, Novikov Pavel, Kuznesova Anastasya
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckystr., 3
e-mail: Novikov.p.ark@yandex.ru

Abstract. The repost considers cyber-resistance as a component of the stability of the information and telecommunications network against computer attacks and also addresses the problem of cyber-resistance.

Keywords: *computer attack; cyber-resistance; enemy; information and telecommunications network.*

В современной войне первоочередными объектами направленного противодействия и поражения стали не войска и оружие, а системы управления противника. Прогнозируемый характер воздействия противника на систему управления и информационно-телекоммуникационную сеть (ИТКС) как ее техническую основу обусловливает появление новых требований к показателям качества функционирования ИТКС.

Использование в ИТКС технологий, средств связи и программного обеспечения иностранного производства, интеграция ИТКС с сетью связи общего пользования (ССОП), а ССОП – с мировым

информационным пространством предопределили смещение акцентов на достижение превосходства над противником на основе применения компьютерных атак (КА) [1].

Результатом воздействия КА являются блокирование управляющей информации и внедрение ложной информации, нарушение установленных регламентов сбора, обработки и передачи информации, отказы, сбои в работе ИТКС ВН, а также компрометация передаваемой (получаемой) информации. В этом случае, КА – один из основных факторов, определяющих устойчивость ИТКС. Прогнозируемый характер воздействия КА на ИТКС обуславливает появление четвертой составляющей устойчивости – киберустойчивости и совокупности качественно новых требований, которым должны соответствовать показатели устойчивости ИТКС. Под киберустойчивостью понимается способность ИТКС обеспечивать управление войсками, силами и оружием в условиях воздействия КА [2].

Для решения проблемы обеспечения киберустойчивости ИТКС необходимо решение следующих задач:

– разработать методику прогнозирования распределения КА по уровням эталонной модели взаимодействия открытых систем (ЭМВОС);

– разработать методику оценки киберустойчивости ИТКС, позволяющую оценивать параметры ИТКС и обосновывать требования к параметрам;

– разработать методику синтеза системы защиты ИТКС [3].

В настоящее время указанные методики разработаны.

Анализ полученных результатов показал, что:

– воздействие КА носит системный характер (комплексно), что требует разработки методики оценки киберустойчивости, которая бы учитывала взаимосвязь традиционных параметров устойчивости (коэффициента связности), вероятностно-временных характеристик комплексных КА и вероятности их воздействия.

– кибеустойчивость и традиционное понятие устойчивости находятся в противоречии. Это позволяет определить оптимальное количество маршрутов для передачи информации и отранжировать маршруты по родам связи и по оперативности управления [4].

– структура системы защиты, должна включать в себя 2 рубежа:

а) сетевой, на базе интегрированных аппаратно-программных средств, реализующих принципы криптографии, межсетевого экранирования, системы разграничения доступа и системы обнаружения вторжений;

б) протокольный.

Заключение. Решение проблемы киберустойчивости позволит повысить устойчивость информационно-телекоммуникационной сети в условиях компьютерных атак.

СПИСОК ЛИТЕРАТУРЫ

1. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия Коцыняк М.А., Лаута О.С., Нечепуренко А.П., Штеренберг И.Г. Труды учебных заведений связи. 2016. Т. 2. № 4. С. 82-87.
2. Применение метода преобразования стохастических сетей для моделирования мобильных банковских атак Саенко И.Б., Лаута О.С., Котенко И.В. Известия высших учебных заведений. Приборостроение. 2016. Т. 59. № 11. С. 928-933.
3. Методика обоснования мер противодействия радиолокационной разведке высокоточного оружия Коцыняк М.А., Карганов В.В., Лаута О.С., Нечепуренко А.П. Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016.№ 9-10 (99-100). С. 54-57.
4. Устройство обнаружения удаленных компьютерных атак Васюков Д.Ю., Коцыняк М.А., Коцыняк М.М., Лаута О.С., Лаута А. С.Патент на изобретение RUS 2540838 03.03.2014

УДК 004.6

СПОСОБ УМЕНЬШЕНИЯ СЛУЖЕБНОГО ТРАФИКА В СЕТИ ПЕРЕДАЧИ ДАННЫХ С КОММУТАЦИЕЙ ПАКЕТОВ

Курашев Заур Валерьевич
Военная академия связи имени Маршала Советского Союза С. М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: Frankilou@yandex.ru

Аннотация. Рассмотрена сеть передачи данных с коммутацией пакетов. Особенности служебного трафика, циркулирующего в сети. Предложен способ уменьшения служебного трафика и выигрыш.

Ключевые слова: *трафик; сеть передачи данных; коммутация пакетов.*

A METHOD FOR REDUCING THE OVERHEAD IN A PACKET DATA NETWORK

Kurashev Zaur
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: Frankilou@yandex.ru

Abstract. Considered a network of data transmission with packet switching. Features of the service traffic circulating in the network. A method for reducing the service traffic and gaining.

Keywords: *traffic; communication network; packet switching.*

Важной подсистемой системы связи является сеть передачи данных (СПД). Для определения места и роли СПД обратимся к РД 45.128 - 2000 «Сети и службы передачи данных». Согласно руководящего документа «Службой ПД называется служба электросвязи, позволяющая пользователям получать от оператора связи набор услуг передачи данных на базе одной или нескольких сетей данных».

Сети ПД не включают в себя оконечное оборудование данных (ООД), в роли которого может выступать ЭВМ.

С распространением ЭВМ повысилась потребность в передаче данных. Протоколы определяют правила обмена на различных уровнях функциональной архитектуры ЭМВОС. Основными аспектами функционирования протокола является эффективность и надежность.

Эффективность связана с производительностью, задержкой, избыточностью и другими количественными характеристиками. Надежность обусловлена правильностью функционирования протокола при передаче данных [1-3]. Основными показателями эффективности традиционно являются производительность и задержка. Производительность оценивается скоростью передачи полезной информации между процессами с учетом всей управляющей информацией и повторных передач. Задержка характеризуется временем начала передачи пакета передатчиком до момента успешного поступления всего пакета в приемник или прихода подтверждения в передатчик при оценке полной задержки.

При передаче больших объемов информации между процессами данные могут иметь различный размер пакета.

В сетях с коммутацией пакетов задержка будет меньше для небольших пакетов, поскольку время передачи на каждом переприемном участке между узлами коммутации пропорционально длине пакета.

Избыточность в коротких пакетах увеличивается, так как каждый пакет содержит заголовок фиксированной длины и для одного и того же объема информации потребуется большой объем обработки и подтверждений.

При коротких пакетах максимальная производительность уменьшается, а эффективность линии возрастает. При использовании длинных пакетов уменьшается избыточность и повышается производительность из-за увеличения задержки [4-6].

Трафик сети передачи данных делится на два класса. К первому классу относится трафик реального времени (передача голосовых сообщений), ко второму классу относятся информационные потоки (пересылка файлов или данных) [7-9].

Способ уменьшения служебного трафика, относящийся к классу информационных потоков, заключается в формировании на передающей стороне сообщения, которое в процессе передачи делится на пакеты различной длины и принимается адресатом на приемной стороне. В свою очередь, адресат, получивший пакет, должен отправить пакет с подтверждением.

Данный пакет он прикрепляет к передаваемому пакету и посылает в канал связи. Вопросы достоверности информации реализованы на другом уровне функциональной архитектуры.

Предлагаемый способ может быть использован в сети передачи данных, который увеличивает пропускную способность линий в два раза, для использования в интересах других услуг.

СПИСОК ЛИТЕРАТУРЫ

1. Протоколы и методы управления в сетях передачи данных: Пер. с англ. / Под ред. Ф.Ф. Куо. -М.: Радиоисвязь, 1985. -480 с.
2. Forney, G.D., Jr., «Convolutional Codes III: Sequential Decoding», Information and Control, 25,pp.267-297, July 1974.
3. Robinson, J.P., «Error Propagation and Definite Decoding of Convolutional Codes», IEEE Transactions on Information Theory, IT-14, pp. 121-128, January 1968.
1. 4. Чуднов А.М., Кирик Д.И., Курашев З.В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений/ Радиотехнические и телекоммуникационные системы. - 2017. -№2. с.41-49.
4. Брунилин А.А., Бирюков М.А., Саенко И.Б. Модель и метод использования онтологий для управления разграничением доступа в едином информационном пространстве // Математические методы в технике и технологиях – ММТТ. 2016. № 6 (88). С. 122-124.
5. Башкирцев А.С., Михайличенко Н.В., Ренсков А.А., Паращук И.Б. Совершенствование объема и номенклатуры множества контролируемых параметров, принадлежащих пространству управления информационными системами и сетями // Успехи современной науки 2017, №1, Т.4, С.46-52.
6. Неижмак А.В., Орешина М.А. Методы защиты облачных хранилищ // Образование и информационная культура: теория и практика. Материалы Межрегионального форума. Под редакцией В.Г. Шубовича. 2016. С. 88-92.
7. Неижмак А.В., Орешина М.А. Направления по защите облачных хранилищ // Информационная и компьютерная безопасность материалы Межрегионального форума «Кибердружина». 2016. С. 30-31.
8. Модель системы связи с управляемыми структурами в конфликтных условиях/ П.Н. Барашков, А.П. Родимов, К.А. Ткаченко, А.М. Чуднов. – Л.: ВАС, 1986. – 52 с.

УДК004.056.53

ПОДХОД К ОЦЕНКЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ОТ ТЕХНИЧЕСКОЙ КОМПЬЮТЕРНОЙ РАЗВЕДКИ

Лаута Олег Сергеевич, Клиншов Илья Андреевич,
Ястребов Владимир Васильевич, Русаков Егор Владимирович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: laos-82@yandex.ru

Аннотация. В докладе представляется один из подходов к оценке защищенности информационно-телекоммуникационной сети специального назначения от технической компьютерной разведки на основе использования оригинальных моделей, учитывающих специфику системы защиты и сценарии действий нарушителей.

Ключевые слова: *техническая компьютерная разведка; компьютерная атака; информационно-телекоммуникационной сеть.*

THE APPROACH TO THE SECURITY ASSESSMENT OF INFORMATION-TELECOMMUNICATION NETWORKS OF SPECIAL PURPOSE FROM TECHNICAL COMPUTER INTELLIGENCE

Lauta Oleg, Klinshov Ilya, Yastrebov Vladimir, Rusakov Yegor
Military Academy of communications
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: laos-82@yandex.ru

Abstract. Theses seem to be one of the approaches to the security assessment of information-telecommunication networks of special purpose from technical computer intelligence through the use of the original models, taking into account the specifics of the protection system and scripts of actions of violators.

Keywords: *technical computer intelligence; computer attack; information-telecommunication network.*

Техническая компьютерная разведка (далее - ТКР) – специально подготовленная, согласованная по цели, месту, времени и формам деятельность, направленная на извлечение и специальную обработку информации из информационно-телекоммуникационной сети специального назначения (ИТКС), а также особенностях их построения и функционирования.

В современных условиях ведение ТКР объективно обладает большим потенциалом по вскрытию функционирующей ИТКС и является предварительным этапом перед воздействием активных компьютерных атак (далее – КА).

В связи с этим возникает необходимость в оценке защищенности ИТКС в условиях КР и КА. Анализ показал, что в большинстве нормативно-правовых документов отсутствует требуемая методика, а в ГОСТе РВ 51987-2002 для оценки защищенности информационных и программных ресурсов рекомендуется разработать оригинальные модели, учитывающие специфику системы защиты и сценарии действий нарушителей.

Для определения оценки защищенности представляется объект ИТКС, основными элементами в котором являются маршрут, направления связи, которые характеризуются вероятностью защищенности.

В ходе анализа ИТКС исследован в обобщенном виде процесс функционирования ИТКС в условиях воздействия КА и были определены основные этапы.

Для осуществления передачи оперативной информации сначала операторы ИТКС входят в связь, на что затрачивается определенное время.

С некоторого времени система информационного воздействия реализует КА за среднее время, которую оператор ИТКС сможет обнаружить за время, определяемое временем реакции системы мониторинга ИТКС ОЗУ.

Обнаружив воздействие КА, оператор ИТКС будет принимать меры по восстановлению связи, в частности, переход на резервные маршруты и принятие других мер. Временные затраты при этом будут определяться оперативностью управления сетью, маршрутом, каналом, средством защиты.

После этого операторы ИТКС восстанавливают связь, на что затрачивается некоторое время, и передача оперативной информации возобновляется.

Среднее время, затрачиваемое на принятие мер защиты, вхождение в связь характеризует реакцию системы управления на воздействие КА, то есть вышеуказанные временные интервалы суммируются.

Среднее время от момента передачи полезной информации до момента воздействия КА назовем временем реакции комплекса технической компьютерной разведки. Реакция комплекса ТКР определяется временем доразведки, необходимым для обнаружения нового маршрута передачи оперативной информации после принятия мер защиты, и временем, необходимым КА для

реализации повторного воздействия на идентифицированный маршрут передачи оперативной информации.

Среднее время реакции комплекса технической компьютерной разведки и воздействия КА характеризует среднее время воздействия противника на ИТКС КА.

Интервал времени, определяемый реакцией КА и затратами времени для реализации мер защиты ИТКС от КА, назовем циклом функционирования комплекса ТКР.

В реальных условиях один цикл работы комплекса ТКР отличается по длительности от другого. Это обусловлено тем, что составляющие циклов – время доразведки, время подготовки комплекса ТКР к работе, принятие мер защиты маршрута от КА, время вхождения в связь и т.д. – имеют, в общем случае, различную длительность в каждом цикле.

С учетом этого возможно определить вероятность защищенности ИТКС от КА как на одном маршруте, так и на маршруте передачи информации, состоящий из нескольких интервалов связи. организованных средствами связи различных родов (радио, радиорелейные, тропосферные, спутниковые и проводные).

Совокупность маршрутов образуют направление связи (НС). Исходя из этого возможно определить вероятность защищенности НС, которое может характеризоваться вероятностью сохранения на НС хотя бы одного маршрута.

Для оценки вероятности защищенности ИТКС необходимо определить вероятность защищенности маршрутов передачи оперативной информации, для чего необходимо определить вероятностно-временные характеристики КА, а также комплекса ТКР.

С этой целью предлагается использовать профильные модели КА (комплекса ТКР) и метод топологического преобразования стохастических сетей (ТПСС).

Результаты расчетов представляются в виде зависимостей: а) зависимость интегральной функции распределения вероятностей от времени работы комплекса ТКР, б) зависимость среднего времени компьютерной разведки комплексом ТКР от вероятности вскрытия ИТКС.

Вышеуказанные результаты дают возможность определить вероятность решения разведывательной задачи комплексом ТКР за время не более заданного, а также среднее время ведения технической компьютерной разведки ИТКС комплексом ТКР. При анализе функции распределения вероятности можно видеть, что при вероятности обнаружения 0,9 и функции распределения вероятности 0,9 время ведения технической компьютерной разведки составляет 100 минут. Для сокращения этих показателей вероятностно-временная характеристика ТКР будет вестись непрерывно и зависит от параметров КА и комплекса ТКР.

Результаты расчета вероятности защищенности ИТКС представлены в виде зависимостей: а) зависимость вероятности защищенности маршрута от среднего времени реакции комплекса технической компьютерной разведки, б) зависимость вероятности защищенности ИТКС от вероятности защищенности НС.

В качестве исходных данных использовались данные, а также значения, соответствующие действующим нормативно-правовым документам (нормативные требования оперативного управления элементами маршрутов и НС ИТКС).

Заключение. Анализ полученных результатов показал, что защищенность ИТКС в условиях КА зависит от времени ведения противником ТКР, являющей предварительным этапом при реализации активных компьютерных атак. Для выполнения общих тактико-технических требований системы специальной связи время ведения противником разведки должно быть не ниже 50 мин.

Однако, в интересах сокращения цикла управления противника ТКР будет вестись непрерывно, в этом случае среднее время будет определяться только подсистемой поиска комплекса ТКР.

Таким образом, полученные результаты позволяют обосновать требования к построению системы защиты в условиях КА и времени реакции системы защиты при ведении противником ТКР.

СПИСОК ЛИТЕРАТУРЫ

1. Исследование функциональной безопасности систем государственного управления. Лепешкин О.М. Инфокоммуникационные технологии. 2007. т. 5. № 3. с. 165-166.
2. Анализ моделей разграничения доступа, реализованных в современных социотехнических системах. Лепешкин О.М., Харечкин П.В. Инфокоммуникационные технологии. 2008. т. 6. № 2. с. 91-93.
3. Методологический подход к оценке безопасности функционирования социальной и экономической системы управления региона. Бурлов В.Г., Лепешкин О.М., Кириллова Т.В. Проблемы экономики и управления в торговле и промышленности. 2013. № 2. с. 99-103.
4. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства. Лаута О.С., Коцыняк М.А., Коцыняк М.М., Васюков Д.Ю., Осадчий А.И., Дементьев В.Е. СПб. ВАС, 2014 – 117 с.
5. Устойчивость информационно-телекоммуникационных сетей. Лаута О.С. Коцыняк М.А., Кулешов И.А. СПб: Издательство Политехнического университета, 2013 – 93 с.

УДК621.391(075.8)

ПРОБЛЕМЫ И ПУТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СПУТНИКОВОЙ СВЯЗИ

Лебеда Евгений Вячеславович, Тарасов Александр Сергеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: zhe48@yandex.ru

Аннотация. В работе рассматриваются вопросы надежной аутентификации пользователей и безопасной передачи информации в системах спутниковой связи. Отмечаются особенности безопасности информации в перенасыщенных системах кодового доступа. Сформулированы пути исследований и дальнейшего развития методов повышения безопасности информации в спутниковой связи.

Ключевые слова: *системы спутниковой связи; перенасыщенные системы с кодовым доступом; криптографические методы.*

PROBLEMSANDWAYS OF SECURITY SATELLITE COMMUNICATIONS

Lebeda Evgeny, Tarasov Aleksandr
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail:zhe48@yandex.ru

Abstract. The article examines the problems of secure user authentication and security of information transmission in satellite communication systems. Features of information security in supersaturated systems with access codes. Formulates ways of research and further development of methods to improve information security in satellite communication.

Keywords: *satellite communication systems; supersaturated systems with access codes; cryptographic methods.*

С развитием космической отрасли, запуском искусственного спутника земли и первым полетом человека в космос появился новый вид связи - спутниковая связь. Бурное её развитие и огромная популярность особенно остро поставили перед разработчиками стандартов спутниковой связи и оборудования вопросы надежной аутентификации пользователей и безопасности передачи информации. Безопасность являлась одним из главных аспектов спутниковой связи с самого ее появления как для операторов, так и для абонентов.

В современном мире вопросы обеспечения безопасности всех сфер жизни деятельности, в том числе безопасности информации являются одними из первостепенных. Часто на это в первую очередь обращают внимание при выборе государственными предприятиями, финансовыми структурами и другими компаниями, успех деятельности которых во многом зависит от обрабатываемой, передаваемой, хранимой ими информации. Поэтому при предоставлении услуг таким пользователям спутниковые операторы уделяют особое внимание защите конфиденциальных данных в своих сетях.

К числу проблем применения для спутниковой связи геостационарных орбит (Thuraya, Inmarsat, Eutelsat) добавляет то, что фиксированное положение искусственного спутника земли на орбите облегчает задачи его уничтожения или нарушения связи искусственными помехами. Об этом было сказано в традиционном ежегодном докладе Министерства связи и массовых коммуникаций Российской Федерации. В нем представлены сведения, что над территорией РФ под видом космического «мусора» размещено около 1000 малоразмерных космических аппаратов с неизвестными функциями [1].

При использовании традиционной мобильной связи или системы Интернет между абонентами всегда есть посредник — провайдер связи, который соединяет звонки и через него проходят все данные. Самое уязвимое место — это прохождение сигнала в дата центре и сотовых вышках. Именно на них проще всего перехватить необходимые данные, при этом абоненты могут даже не подозревать об этом. На данный момент только системы спутниковой связи предлагают минимальное участие "посредника" и наземных сетей при связи между абонентами. При передаче информации по каналам спутниковой связи от одного телефонного аппарата к другому сигнал без ретрансляции земной станции проходит через спутники на телефонный аппарат вызываемого абонента. При этом наземные станции (дата-центр), получают только технические данные, такие как: длительность вызова и геопозиция с точностью до континента. Более того, сигнал от спутникового телефона не конусный (как на мобильных телефонах), а направленный, что делает более затруднительным съём информации с телефонного аппарата направленными спецсредствами. Таким образом, обмен информацией по спутниковым каналам между двумя абонентами делает данный вид связи наиболее защищенным по сравнению с другими видами. Однако, в современном информационно-вычислительном мире ни один вид связи, в том числе и спутниковая, не дает гарантии, что все данные, которые пользователь загружает через спутниковый ретранслятор, ни могут быть перехвачены посторонними лицами. В канале передачи,

между передатчиком и приемником, сообщение может быть перехвачено злоумышленником, который получает несанкционированный доступ к его содержанию, и может либо исказить сообщение, либо произвести замену исходного сообщения ложным. Первая задача решения проблемы соответствует классическому шифрованию, вторая – работе в условиях преднамеренных помех, третья – электронной подписи [2].

Вопрос безопасности информации актуален и для перенасыщенных систем с кодовым доступом используемых в спутниковой связи, т.к. избыточность абонентов вводит более жесткие требования к помехозащищенности и отношению сигнал/шум. Превышение количеством абонентов сигнального пространства осуществляется с помощью оптимизации сигнатурных ансамблей по критерию минимума расстояния. Именно поэтому, любое внесение помехи или искажения N-мерного сигнального пространства может привести к срыву сеанса связи или потере пакета сообщения [3].

Криптографические методы являются одним из самых очевидных и эффективных способов предотвращения несанкционированного доступа к каналам связи и дублирования аппаратов связи. Основным способом обеспечения безопасности передачи данных в беспроводном спутниковом канале является применение аппаратно-программных средств защиты данных. Во-первых, весь обмен информацией с внешними сетями и Internet контролируется в соответствии с заданной политикой безопасности на пограничных маршрутизаторах и межсетевом экране оператора. Во-вторых, передаваемые данные шифруются с помощью фирменных алгоритмов криптозащиты производителя спутникового оборудования. В-третьих, постоянный сбор статистики по работе сети и серверов позволяет технической службе эффективно отслеживать и корректировать функционирование сети в любое время суток.

Шифрование данных в спутниковом канале осуществляется при участии как спутниковых терминалов на стороне клиента, так и специализированных высокопроизводительных серверов на центральной управляющей станции (ЦУС) оператора. На специальном сервере оператора размещается защищенная база данных ключей шифрования и сеансовых ключей всех спутниковых терминалов. Чтобы терминал смог работать в сети оператора, информация в базе ключей оператора должна соответствовать аппаратному ключу, который хранится на интегральной схеме терминала. Это исключает несанкционированное подключение терминалов «чужого» оператора. За генерацию ключей и их распространение отвечает компания-производитель спутникового оборудования. Терминалы изготавливают таким образом, чтобы они были защищены от извлечения ключей шифрования, воздействия любых внешних сигналов, а также от вскрытия оборудования для анализа.

На серверах ЦУС для межсерверного сетевого взаимодействия операторы часто используют модифицированные транспортные протоколы. Это делается в целях обеспечения полного контроля за серверными сетевыми интерфейсами, а также для защиты от несанкционированного доступа к ним. Каждый сервер имеет «горячий» резерв — отдельно стоящий идентичный сервер, который берет на себя всю работу в случае выхода из строя основного устройства. Кроме того, сетевое взаимодействие оборудования логически разделено на виртуальные сети по технологии VLAN (IEEE 802.1Q), чтобы данные для управления и контроля были изолированы от пользовательских. В результате атаки на сеть оператора со стороны клиентов или из Internet становятся невозможными, а распространение вирусов в сети блокируется.

Спутниковые абонентские терминалы имеют необходимый набор средств для обеспечения как собственной безопасности, так и для защиты подключенных к ним сетей. Главным инструментом, является сетевой фильтр. Его функций достаточно, чтобы исключить большинство атак по портам и протоколам на сети клиентов через спутниковые каналы связи. Расширенные возможности по регистрации различных ошибок, попыток несанкционированного доступа и взлома предоставляет сервис генерации событий. Информация о событиях автоматически передается на центральный пульт управления ЦУС оператора. Для более детального анализа работы терминала используются записи в журнале событий. Управлять спутниковыми терминалами и изменять их конфигурации разрешается только компетентным техническим специалистам ЦУС оператора. Обычно они используют программный комплекс, разработанный производителем спутникового оборудования. Посредством этого ПО эффективно решается большая часть задач по защите информации в канале: регистрация новых терминалов, контроль их состояния и доступа, управление информацией о ключах.

Именно из-за особенности работы спутниковой связи её используют не только как связь в удаленных местах планеты, где нет покрытия наземными сетями, но и как безопасный канал связи и телефон, защищенный от прослушивания. Любые операции по криптоанализу спутниковой связи являются дорогостоящими и доступными практически только спецслужбам.

СПИСОК ЛИТЕРАТУРЫ

1. Е.Е. Исаков. Основные принципы построения устойчивой военной связи и возможные способы их реализации. // СПб.: ВАС. 2015., С. 259-263;
2. В. Вишневский, С. Портной, И. Шахнович. Энциклопедия WiMAX. Путь к 4G. // ЗАО «РИЦ «Техносфера»., С. 57- 59;
3. Ипатов В.П. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. // Москва. Техносфера, С. 279-288.

УДК 519.876.5

РАЗРАБОТКА НАУЧНО-МЕТОДИЧЕСКОГО АППАРАТА ИДЕНТИФИКАЦИИ И ПРОГНОЗИРОВАНИЯ ЭВОЛЮЦИИ МЕЖЭТНИЧЕСКИХ И МЕЖКОНФЕССИОНАЛЬНЫХ КОНФЛИКТОВ, ВОЗНИКАЮЩИХ В РЕЗУЛЬТАТЕ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Лозовский Владимир Валерьевич, Винокуров Александр Владимирович,
Галицкий Валерий Андреевич
Краснодарское высшее военное училище им. генерала армии С.М. Штеменко
Россия, г. Краснодар, ул. Красина, 4
e-mail: lozovskiy_v_v@rambler.ru

Аннотация. Обосновывается необходимость разработки научно-методического аппарата идентификации и прогнозирования эволюции межэтнических и межконфессиональных конфликтов, возникающих в результате информационного противоборства, формулируются тема, объект, предмет и цель проводимого научного исследования, а также ставятся частные научные задачи исследования.

Ключевые слова: *информационное противоборство; информационно-психологические операции, межэтнические и межконфессиональные конфликты.*

DEVELOPMENT OF THE SCIENTIFIC AND METHODOLOGICAL APPARATUS FOR IDENTIFICATION AND FORECASTING THE EVOLUTION OF INTER-ETHNIC AND INTER-CONFLICTIONAL CONFLICTS ARISING FROM THE RESULT OF INFORMATION INFECTIONS

Lozovskiy Vladimir, Vinokurov Aleksandr, Galickiy Valeriy
The Krasnodar Higher Military School named after army General S.M. Schtemenko
Russia, Krasnodar, Krasina str., 4
e-mail: lozovskiy_v_v@rambler.ru

Abstract. The author substantiates the necessity of developing a scientific and methodical apparatus for identifying and forecasting the evolution of interethnic and interconfessional conflicts arising as a result of information confrontation, formulating the theme, object, subject and purpose of the scientific research being carried out, as well as individual scientific research tasks.

Keywords: *information confrontation; information-psychological operations; interethnic and interconfessional conflicts.*

Мир был и остается многонациональным и, несмотря на высокую интенсивность процесса глобализации, трудно предположить, что он перестанет быть таковым в будущем. Проведенный анализ позволяет сделать вывод, что подавляющее большинство стран нашей планеты являются многонациональными. Полиэтничность государства может стать источником многих проблем: социальных, политических, культурных, лингвистических и т.п. Так, например, Д. Хоровиц считает, что люди, для того чтобы защитить свои интересы, образуют группы, которые предпринимают коллективные действия, в том числе и для защиты от других групп [1]. Группы, формируемые по национальному признаку, безусловно, не являются исключением. В этом случае, этническое сознание, будучи политическим или социальным явлением, может рассматриваться, как «форма конфликта» [2].

Проблема межнациональных отношений актуальна и для Российской Федерации. По данным переписи 2002 и 2010 годов национальный состав Российской Федерации был представлен более, чем 194 народами. При этом русские составляют 79,83% от общего числа. То есть, численность нерусского населения составляет около 30 миллионов человек, при этом численность 8 народов, каждый из которых компактно проживает на определенной территории, что немаловажно, составляет более 10% от всего населения Российской Федерации.

Межнациональные отношения являются весьма непростой областью для изучения, а тем более возможного регулирования. Как и в любой другой области социального бытия, сфера межнациональных отношений имеет свои законы, закономерности и тенденции, игнорирование которых может привести к самым трагичным последствиям [3]. Влияние межнациональных отношений на обороноспособность и социально-экономическое положение государства, а стало быть, и государственную безопасность в целом, может быть существенным.

Поэтому анализ возможных направлений целенаправленного воздействия на многочисленные этнические микро и макрогруппы нашего государства, а, главное, анализ возможных последствий таких воздействий, представляют собой актуальную государственную задачу. Основная цель решения данной задачи может быть сформулирована, как определение основных механизмов, посредством которых осуществляется воздействие на межэтнические отношения, и на основе этого разработать универсальные методы идентификации этнического сепаратизма на ранних этапах его зарождения.

Говоря о роли межнациональных отношений в структуре государственной безопасности, уместно вспомнить римский принцип государственной власти «разделяй и властвуй», который нередко используется в отношении государств, состоящих из неоднородных социальных групп. Согласно этому принципу, лучший метод управления таким государством – разжигание и использование вражды между его составными частями.

Формировать различные части внутри государства, которые впоследствии будут создавать социальные неоднородности, которые во имя сознательно формируемых извне идей станут уничтожать друг друга, разрушая государство, можно различными методами и средствами. В ходе данных исследований в качестве основного критерия формирования социальной неоднородности рассматривается этническое разнообразие государств.

По мнению авторов, данный критерий является наиболее надежным, с позиции заинтересованной воздействующей стороны, и бескомпромиссным, с точки зрения протекания дестабилизирующих последствий. Под влиянием некоторых возмущающих воздействий этнические группы превращаются в "конфликтующие группы", а этничность, или национальный вопрос, способны "разбудить" этнополитический конфликт [2]. В настоящее время в Краснодарском высшем военном училище имени генерала армии С.М. Штеменко проводится научное исследование на тему: «Разработка научно-методического аппарата идентификации и прогнозирования эволюции межэтнических и межконфессиональных конфликтов, возникающих в результате информационного противоборства (ИП)». В качестве возмущающего воздействия, формирующего негативные межэтнические и межконфессиональные отношения, рассматриваются методы и средства информационно-психологических операций, как составной части ИП. Актуальность роли информационно-психологической составляющей информационной безопасности подтверждается соответствующими положениями Доктрины информационной безопасности РФ [4].

Объект исследования: межэтнические и межконфессиональные конфликты.

Предмет исследования: влияние информационно-психологических операций, как вида ИП, на формирование и развитие межэтнических и межконфессиональных конфликтов. Проблема: необходимость идентификации и прогнозирования формирования и развития межэтнических и межконфессиональных конфликтов, возникающих в результате реализации мероприятий, проводимых в рамках ИП, как одной из угроз национальной безопасности РФ.

Цель исследования: разработать методы, модели, алгоритмы, обеспечивающие идентификацию и прогнозирование основных этапов эволюции межэтнических и межконфессиональных конфликтов, возникающих в результате информационного противоборства.

Для достижения поставленной цели решаются и планируются к решению следующие задачи:

– анализ причин возникновения и основных этапов эволюции межэтнических и межконфессиональных конфликтов с целью формирования исходных данных для построения концептуальной модели;

– разрабатываются математические модели основных этапов эволюции межэтнических и межконфессиональных конфликтов, возникающих в результате ИП;

– разрабатывается динамическая модель эволюции межэтнических и межконфессиональных конфликтов, возникающих в результате ИП;

– разрабатываются методы мониторинга, идентификации и прогнозирования основных этапов эволюции межэтнических и межконфессиональных конфликтов;

– разрабатывается экспертная система контроля и прогнозирования формирования и развития межэтнических конфликтов;

– разрабатываются алгоритмы принятия управленческих решений на основе методов идентификации, мониторинга и прогнозирования основных этапов эволюции межэтнических и межконфессиональных конфликтов, возникающих в результате ИП.

Таким образом, с уверенностью можно сказать, что проводимые научные исследования влияния информационно-психологических операций на формирование и развитие межэтнических и межконфессиональных конфликтов, являются актуальными, а разработанный научно-методический аппарат идентификации и прогнозирования эволюции межэтнических и межконфессиональных конфликтов может быть использован в управленческой и законотворческой деятельности органов государственной власти.

СПИСОКЛИТЕРАТУРЫ:

1. Horowitz D. Ethnic Groups in Conflict.-Berkeley, 1985.
2. Малышева Д.В. Феномен этносепаратизма на Кавказе и мировой опыт // Региональные конфликты в Азии и Северной Африке. - М., 2011. - С. 267-282.
3. Козырев М.С. Межнациональные отношения и их влияние на обороноспособность современной России: социально-философский анализ // Диссертация на соискание учёной степени кандидата философских наук: 09.00.11. Москва, 2007. - 216 с.
4. Доктрина информационной безопасности Российской Федерации: [утверждена указом Президента Российской Федерации от 5 декабря 2016 г. № 646].

УДК 004.056.57

АНАЛИЗ СПОСОБОВ МОДЕЛИРОВАНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ В КИБЕРПРОСТРАНСТВЕ

Львова Наталия Владиславовна, Бречко Александр Александрович, Баленко Ольга Александровна
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: lvovanv84@mailr.ru, sashabreck27@gmail.com

Аннотация. Проведен анализ существующих способов моделирования конфликтных ситуаций в киберпространстве. Проанализированы вопросы информационной безопасности, требующие решения для обеспечения динамической защиты информационно-телекоммуникационной сети.

Ключевые слова: *киберпространство; моделирование; информационная безопасность; конфликтная ситуация.*

MODELING WAYS ANALYSIS OF CONFLICT SITUATIONS IN CYBERSPACE

Lvova Nataliya, Brechko Alexandr, Balenko Olga
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: lvovanv84@mailr.ru, sashabreck27@gmail.com

Abstract. Here was done the analysis of existing modeling ways of conflict situations in cyberspace. The issues of information security, which require solutions for information security, are analyzed

Keywords: *cyberspace; cyberspace; modeling; information security; conflict situations.*

В работе под киберпространством понимается масштабируемая, неоднородная искусственная система с сетецентрическим управлением, обеспечивающая процессы генерации, передачи, хранения, обработки и потребления информации, в интересах разнородных, в том числе антагонистических систем управления, в которой свойства (характеристики) элементов зависят от собственных характеристик, объема и свойств реализуемых процессов в интересах внутренних и внешних потребителей [1].

Переход от первичных и вторичных сетей к цифровой транспортной и мультисервисной сетям, позволил уйти от предоставления абонентам отдельных видов связи к предоставлению интегрированных услуг связи.

В настоящее время для предоставления интегрированных услуг абонентам информационно-телекоммуникационная сеть (ИТКС), в условиях ограниченности своих ресурсов, использует ресурсы единой сети электросвязи (ЕСЭ), которая является частью глобальной телекоммуникационной сети, ресурсы которой являются общими с нарушителем.

Происходит интеграция сетей, а также конвергенция сетей и услуг, обеспечивая абонентам доступ к любой услуге из любой сети. Все это привело к принципиальным изменениям построения ИТКС: средствами ИТКС осуществляется только организация сети доступа и привязки к ЕСЭ РФ; используется телекоммуникационное оборудование, производителями которого являются иностранные государства.

Вышеописанная ситуация позволяет нарушителю применять различные программные воздействия на ИТКС.

Комплексный характер программных воздействий на ИТКС, особенности развития стратегии, тактики действий и технического оснащения злоумышленников, приводят к существенному ужесточению требований, предъявляемых к системе защиты ИТКС.

Решениями вышеописанной проблемы являются:

– снижение воздействия нарушителя на ИТКС;
– полное исключение воздействий нарушителя (вследствие использования средств защиты);
– опережение воздействий нарушителя во времени.

Таким образом, общее время цикла защиты сетевых элементов ИТКС от программных воздействий нарушителя должно быть меньше либо равно общему времени цикла реализации воздействий нарушителя на сетевые элементы ИТКС. Возникает необходимость в разработке способа моделирования и моделей, позволяющих уменьшить общее время цикла защиты элементов ИТКС.

В связи с этим существует необходимость в разработке способов моделирования и комплекса динамических моделей конфликтных ситуаций между системой защиты ИТКС и системой воздействий нарушителя, позволяющих осуществить интеллектуальную поддержку руководителям при принятии решения о необходимых способах динамической защиты ИТКС в реальном масштабе времени, которая учитывает условия ведения информационного противоборства.

Такая модель в общем виде описывает две конфликтующие ИТКС (динамическая система защиты и динамическая система, создающая программные воздействия) и общую физическую среду, через которую обеспечивается взаимодействие между ними [3].

Анализ работ в области моделирования систем связи показал, что:

– конфликт систем защиты и воздействия рассматривается на одном уровне функционирования этих систем – физическом, канальном, сетевом, транспортном уровнях OSI;

– не рассматривают взаимодействие нарушителя и средств защиты в качестве конфликта;

– не учитывают тот факт, что объектами информационного противоборства являются сложные иерархические информационно-управляющие системы;

– работы в области анализа функционирования комплексов связи и управления как многоуровневых иерархических систем - не рассматриваются конфликтные ситуации характерные для информационного противоборства;

– моделируемые системы являются статическими.

Известные работы в области информационного конфликта основываются на научно-методическом аппарате:

– теории активных систем;
– теории игр;
– марковских процессов;
– многоагентных интеллектуальных систем;
– теории сетей Петри;
– теории автоматов;
– вероятностные сети;
– теории динамических систем;
– теории сложных иерархических систем [4,5].

Таким образом, существующие традиционные модели и способы не позволяют в полной мере описать изменившиеся условия построения, функционирования ИТКС, соответственно, должны быть пересмотрены (разработаны), с учетом изменившейся обстановки [6].

Разработка способов моделирования и комплекса динамических моделей конфликтных ситуаций в киберпространстве между системой защиты ИТКС и системой воздействий нарушителя с учетом изменившихся условий построения и функционирования ИТКС является актуальной задачей и может быть решена с использованием метода имитационного моделирования, которое позволит:

– проводить эксперименты с еще только проектируемыми системами и изучать их;

– учитывать различные случайные процессы, возможные при функционировании ИТКС и в условиях программных воздействий нарушителя;

– легко изменять значения параметров и начальных условий;

– исследовать качество услуг, предоставляемых абонентам системы связи и поддержания его стабильности в каждой из конфликтных ситуаций;

– анализировать поведение сети при различных решениях по построению системы управления, изменять структуру сети;

– повторное использование уже созданных и подтвердивших свою работоспособность моделей;

– с приемлемыми трудозатратами осуществлять программную реализацию имитационной модели конфликтных ситуаций между ИТКС и средствами воздействия нарушителя [7].

СПИСОК ЛИТЕРАТУРЫ

1. Стародубцев Ю.И. Управление качеством информационных услуг / Ю.И. Стародубцев, А.Н. Бегаев, М.А. Давлятов; под общ. Ред. Ю.И. Стародубцева. – СПб. : Изд-во Политехн. Ун-та, 2017. – 454 с.
2. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 83-89.
3. Паршуткин А В. Концептуальная модель взаимодействия конфликтующих информационных и телекоммуникационных систем Вопросы кибербезопасности. 2014. №5(8). С. 2-6.
4. Макаренко С.И. Динамическая модель системы связи в условиях функционально–разноуровневого информационного конфликта наблюдения и подавления. // Системы управления, связи и безопасности. 2015. № 3. С. 122-185.
5. Саенко И.Б., Бирюков М.А., Ефимов В.В., Ясинский С.А. Модель администрирования схем разграничения доступа в облачных инфраструктурах // Информация и космос. 2017. № 1. С. 121-126.
6. Стародубцев Ю.И., Бречко А.А., Львова Н.В. Необходимость оценки защищенности системы связи от средств информационной борьбы в современных условиях. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1201.
7. Модель таргетированной кибернетической атаки. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 90-98.

УДК 620.92

ИСПОЛЬЗОВАНИЕ ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ КОНТРОЛЛЕРОВ ДЛЯ ИЗМЕРЕНИЯ ПАРАМЕТРОВ НАПРЯЖЕНИЯ В СЕТЯХ ЭЛЕКТРОСНАБЖЕНИЯ

Мель Михаил Игоревич, Щукин Андрей Владимирович
Военная академия связи имени Маршала Светского Союза С.М. Буденного
Россия, Санкт-Петербург, пр. Тихорецкий,3
e-mail: vas@mil.ru

Аннотация. В докладе обоснована экономическая целесообразность создания вольтметра переменного напряжения на основе программируемого логического контроллера, описана его схема и процесс работы.

Ключевые слова: *моделирование; напряжение; контроллер; вольтметр.*

THE USE OF PROGRAMMABLE LOGIC CONTROLLERS FOR VOLTAGE MEASUREMENT IN POWER SUPPLY NETWORKS

Mel'Mikhail, Shukin Andrey
The S.M.Budjonny Military Academy of the Signal Corps
St. Petersburg, Tichorezki pr., 3
e-mail: vas@mil.ru

Abstract. The report substantiates the economic feasibility of establishing a voltmeter the AC voltage based on a programmable logic controller, described its circuit and working process

Keywords: *modeling; voltage; controller; voltmeter.*

Одним из факторов обеспечения безопасности и эффективной работы объектов МО РФ является исправная работа сетей электроснабжения. Для обеспечения постоянной исправной работы сетей электроснабжения необходимо постоянно осуществлять мониторинг их параметров и в случае отклонения параметров от нормируемых значений принимать неотложные меры по их восстановлению. В настоящее время технические средства позволяют осуществлять постоянный автоматический мониторинг таких параметров и в случае отклонений предупреждать об этом персонал. Таким образом, разработка систем удаленного мониторинга является актуальной задачей обеспечения безопасности и эффективной работы объектов МОРФ.

В общем случае система удаленного мониторинга включает в себя следующие составные части: оборудование осуществляющее мониторинг параметров электрической сети, оборудование осуществляющее передачу данных от устройства, осуществляющего мониторинг, к серверу, сервер содержащий базу данных с измеренными ранее показателями, рабочее место оператора с пользовательским интерфейсом.

В процессе работы были проанализированы несколько вариантов исполнения системы удаленного мониторинга в части снятия показаний и передачи данных не сервер.

Первый вариант: использование мультиметра и преобразователя интерфейса. Общая стоимость 17 000 руб. Преимущества: относительно недорогой вариант, мониторинг большинства показателей качества электроэнергии. Недостатки: отсутствие возможности измерения дозы фликера и гармонических составляющих.

Второй вариант: использование анализатора параметров трехфазной сети и преобразователя интерфейса. Общая стоимость 25 000 руб. Преимущества: измерение всех параметров качества электроэнергии. Недостатки: увеличенная стоимость.

Третий вариант: использование мультиметра с Ethernet интерфейсом. Общая стоимость 39 000 руб. Преимущества: измерение всех показателей качества электроэнергии, исключение из схемы преобразователя интерфейса. Недостатки: высокая стоимость.

Четвертым вариантом является создание анализатора качества электроэнергии на основе программируемого логического контроллера.

Для примера рассмотрим использование микроконтроллера Arduino UNO. Данная модель взята по причине её широкой распространенности, большого количества доступных расширяющих модулей и материалов по настройке микроконтроллера. Стоимость Arduino UNO совместно с Ethernet модулем составит приблизительно 2000 руб.

Для осуществления замеров в сети необходимо понизить сетевое напряжение, до напряжения, не превышающего 5 В. Для этой задачи подходит понижающий трансформатор фирмы IEK ЯТП-220/12/0,25 имеющий 220 В на первичной обмотке и 12 В на вторичной. Преимущества использования трансформатора заключаются в простоте его конструкции и, как следствие, надежности, а также в наличии гальванической развязки между силовой и измерительной цепью, что обеспечивает безопасность измерительного оборудования. Далее при помощи делителя напряжения на резисторах понижаем 12 вольт до 5 В. Стоимость трансформатора составляет 2000 руб., стоимость компонентов для реализации схемотехнических решений не превысит 1000 руб.

Общая стоимость оборудования необходимого для реализации анализатора качества электроэнергии на основе микроконтроллера составит приблизительно 5000 руб., что значительно дешевле всех ранее рассмотренных вариантов.

Основным препятствием на пути создания вольтметра переменного напряжения на основе Arduino является то, что аналоговый пин контроллера измеряет напряжение только в пределах от 0 до 5 В. Соответственно отрицательные значения напряжения контроллер не распознает [1].

Решением данной задачи является смещение синусоиды переменного напряжения вверх по оси у, до тех пор, пока значения напряжения не перестанут принимать отрицательные значения.

Физически эта задача решается сложением постоянного и переменного тока.

Как было сказано выше на выходе из трансформатора мы получаем переменное напряжение с действующим значением 1 В, амплитудное значение составит соответственно 1,41 В. Если учесть диапазон измерения напряжения контроллером (0…5В) и принять значение постоянной составляющей 2,5 В, то минимальное значение на пине микроконтроллера будет 1,09 В, максимальное 3,91 В. Данные значения входят в диапазон напряжений измеряемый на пине микроконтроллера.

Далее в программном обеспечении самого контроллера напряжению на пине ставится в соответсвие напряжение на источнике, после чего оно выводится на экран LCD1 [2].

Экран подключается к дискретным пинам контроллера. На схеме V3 источник питания экрана LCD1, RV1 – реостат при помощи которого регулируется яркость экрана.

На экран выводятся мгновенное, максимальное и минимальное значения напряжений.

Таким образом, использование программируемых логических контроллеров имеет ряд преимуществ:

Цена данных устройств значительно ниже, чем у готовых аналогов;

Относительная простота конструкции не требует большого числа ресурсов на создание прибора;

Имеется возможность дальнейшего развития функционала прибора.

СПИСОК ЛИТЕРАТУРЫ

1. Мелик-Шахназаров, А. М. Измерительные приборы со встроенными микропроцессорами / А.М. Мелик-Шахназаров, М.Г. Маркатун, В.А. Дмитриев. - М.: Энергоатомиздат, 2000. - 240 с.

2. Улли, Соммер Программирование микроконтроллерных плат Arduino/Freeduino / Соммер Улли. - М.: БХВ-Петербург, 2017. - 328 с.

УДК621.391(075.8)

ВОПРОСЫ ЗАЩИТЫ ИНТЕРЕСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Неижмак Алексей Владимирович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: leshechka_87@mail.ru

Аннотация. В докладе описывается подход к созданию системы информационного противоборства с участием патриотически настроенных граждан с целью повышения степени защиты интересов Российской Федерации в информационном пространстве. Система представляет собой формирование граждан, обладающих знаниями и умениями в области информационных технологий, которые содействуют их взаимодействию с силовыми ведомствами и провайдерами.

Ключевые слова: *киберсанкции; кибераграссия; информационная безопасность; информационная работа; замаскированные выходы.*

QUESTIONS OF PROTECTING THE INTERESTS OF THE RUSSIAN FEDERATION IN THE INFORMATION SPACE

Neizhmak Alexey
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: leshechka_87@mail.ru

Abstract. The report describes the approach to creating an information confrontation system with the participation of patriotic citizens in order to improve the degree of protection of the interests of the Russian Federation in the information space. The system is the formation of citizens with knowledge and skills in the field of information technology, which facilitate their interaction with law enforcement agencies and providers.

Keywords: *cybersanctions; cyberragession; information security; information work; disguised outputs.*

В современных условиях информационная составляющая ведения боевых действий имеет значительно больший вес, чем раньше. Поэтому для успешного ведения "кибервойны" и отражения "кибератак" необходимо иметь достаточное количество сил и средств.

Опыт последних конфликтов показывает, что невозможно полностью изолировать информационное пространство страны. Такая изоляция скорее приведет к информационному поражению, чем к обеспечению нормального функционирования всех информационных средств. Более того, во время "кибервойны" будут активизироваться не только атакующие "снаружи". Проявят активность и "внутренние ИТ киберсаботажники" и "кибер-лжепатриоты".

Существующего количества специалистов по информационной безопасности (ИБ) силовых министерств и ведомств будет явно недостаточно для борьбы с "киберврагом," несмотря на "киберзакладки", которые тоже начнут активно функционировать.

Насколько граждане нашей страны готовы к противостоянию в условиях внутренней и внешней киберагрессии? Ответ на этот вопрос не столь очевиден. Например, вопросы противодействия терроризму для простых граждан освящены с помощью пропаганды и средств наглядной агитации. Личный состав ВС РФ, сотрудники МЧС и МВД подготавливаются к реальным действиям в ходе тренировок и учений. А вот системы подготовки граждан к информационному противодействию не существует [1].

Опыт последних событий в европейской части показывает, что часть патриотически настроенных граждан, обладающая знаниями в области информационных технологий (ИТ), способна оказать достаточно большое информационное противодействие. Но эти действия осуществляются спонтанно, разрозненно, т.к. не координируются государством, следовательно, их эффективность окажется низкой.

Обозначенная выше проблема заключается в том, что государство не имеет на данный момент механизма, повышающего эффективность действий граждан, искренне желающих внести существенный вклад в информационное противоборство [2].

Для решения проблемы предлагается создание в стране подготовленных формирований из наиболее ИТ-грамотных и патриотически настроенных граждан, которые получат название "киберпополнение".

Создание подготовленного и эффективного формирования должно предусматривать решение следующих задач:

– разработка нормативных документов,
– создание материальной базы,
– подготовка провайдеров,
– создание системы подготовки участников формирований.

Решение поставленных задач должно быть осуществлено заранее. На предлагаемые формирования можно возложить и решение текущих задач по обеспечению информационной поддержки функционирования государства.

Решением трех первых задач должны заниматься соответствующие силовые ведомства. Задача подготовки квалифицированного "кибероподчения" должна решаться на базе учебных заведений с привлечением сотрудников отделов ИБ силовых структур [3].

Создание системы подготовки квалифицированного персонала должно предусматривать:

– формирование "киберотрядов",
– проведение "киберсборов" на базе ВУЗов под руководством сотрудников отделов ИБ силовых ведомств,
– проведение заочных и очных "кибертренировок" с привлечением провайдеров,
– обеспечение планомерной "киберпрофилактической" работы.

Руководителями формирований должны являться штатные сотрудники служб информационной безопасности силовых ведомств. А участниками формирований должны стать наиболее подготовленные, патриотически настроенные граждане. Необходимо разработать несколько уровней информационной работы – от словесной поддержки соответствующего контента до его участия, например, в организации массированных кибератак. В результате обучения, основываясь на его результатах,

– ранжируются члены согласно их уровню компьютерной грамотности,
– формируются группы "кибердобровольцев" согласно ролям и психологической совместимости.

Группы должны формироваться по территориальному признаку с мобильным оснащением их соответствующим аппаратным и программным оборудованием.

Возможно формирование распределенных групп не по территориальному признаку, а в зависимости от решаемых задач [4].

Для обеспечения деятельности предлагаемых объединений, необходимо предусмотреть возможность их работы в выделенной закрытой сети, а также сам факт предоставления им выхода в информационное пространство с помощью "замаскированных выходов" (работа под ложными ip-

адресами, формирование обманных сетей и т.д.), обеспечиваемых провайдерами в соответствии с разработанными заранее нормативными документами.

Создание подобной системы позволит обеспечить более качественную и эффективную защиту интересов граждан Российской Федерации в мировом информационном пространстве [5].

СПИСОК ЛИТЕРАТУРЫ

1. Исаев Г.Н. Информационные технологии: Учебное пособие / Г.Н. Исаев. − М.: Омега-Л, 2013. –464 с..
2. Чуднов А.М., Кирик Д.И., Курашев З.В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений / Чуднов А.М., Кирик Д.И., Курашев З.В. / Радиотехнические и телекоммуникационные системы. - 2017. -№2. с.41-49
3. Бирюков М.А. Разработка модели нарушителя правил разграничения доступа к единому информационному пространству // Математические методы в технике и технологиях – ММТТ. 2017. Т. 3. С. 107-110.
4. Паращук И.Б., Башкирцев А.С., Михайличенко Н.В. Анализ уровней и видов неопределенности, влияющей на принятие решений по управлению информационными системами // Информация и космос 2017 № 1 С.112-120.
5. Калюка В.И., Овсянников С.Н., Сапунова Л.П. Оптимизация локального ресурса пропускной способности сети широкополосного радиодоступа// Наукоемкие технологии в космических исследованиях Земли. 2016. Т.8. №3, С.35-40.

УДК621.391(075.8)

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Мехряков Александр Владимирович, Шибанов Данил Сергеевич, Трифонов Павел Валерьевич,
Бирюков Михаил Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: mydearemmawatson@gmail.com, shibanovd94@mail.ru, deft1234@mail.ru

Аннотация. В работе рассматриваются основные способы защиты данных от несанкционированного доступа, перечислены меры защиты информационной безопасности компьютерных систем.

Ключевые слова: *информационная безопасность; несанкционированный доступ; компьютерные преступления; меры защиты информации.*

PROTECTION OF INFORMATION FROM UNAUTORIZED ACCESS

Mekhryakov Alexandr,Shibanov Danil, Trifonov Pavel, Birukov Mikhail
S.M. Budjonny Military Academy of the Signal Corps
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: mydearemmawatson@gmail.com, shibanovd94@mail.ru, deft1234@mail.ru

Abstract. In the paper the main ways of data protection from unauthorized access are considered, Measures of information security protection of computer systems are listed.

Keywords: *Information security; unauthorized access; computer crimes; Information security measures.*

Использование компьютеров и автоматизированных технологий приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Электронные средства хранения даже более уязвимы, чем бумажные: размещаемые на них данные можно и уничтожить, и скопировать, и незаметно видоизменить.

Число служащих в организации, имеющих доступ к компьютерному оборудованию и информационной технологии, постоянно растет. Доступ к информации больше не ограничивается только узким кругом лиц из верхнего руководства организации. Чем больше людей получает доступ к информационной технологии и компьютерному оборудованию, тем больше возникает возможностей для совершения компьютерных преступлений.

Признаки компьютерных преступлений: неавторизованное использование компьютерного времени; неавторизованные попытки доступа к файлам данных; кражи частей компьютеров; кражи программ; физическое разрушение оборудования; уничтожение данных или программ; неавторизованное владение дискетами, лентами или распечатками.

Защита информации – это деятельность по предотвращению утраты и утечки защищаемой информации.

Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода.

Информационная безопасность дает гарантию того, что достигаются следующие цели:

– конфиденциальность критической информации;

– целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода);

– доступность информации, когда она нужна;

– учет всех процессов, связанных с информацией.

Под критическими данными понимаются данные, которые требуют защиты из-за вероятности нанесения ущерба и его величины в том случае, если произойдет случайное или умышленное раскрытие, изменение, или разрушение данных. К критическим также относят данные, которые при неправильном использовании или раскрытии могут отрицательно воздействовать на способности организации решать свои задачи; персональные данные и другие данные, защита которых требуется указами Президента РФ, законами РФ и другими подзаконными документами.

Любая система безопасности, в принципе, может быть вскрыта. Эффективной считают такую защиту, стоимость взлома которой соизмерима с ценностью добываемой при этом информации.

Существует четыре уровня защиты компьютерных и информационных ресурсов:

– предотвращение предполагает, что только авторизованный персонал имеет доступ к защищаемой информации и технологии.

– обнаружение предполагает раннее раскрытие преступлений и злоупотреблений, даже если механизмы защиты были обойдены.

– ограничение уменьшает размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению.

– восстановление обеспечивает эффективное воссоздание информации при наличии документированных и проверенных планов по восстановлению.

Меры защиты - это меры, вводимые руководством, для обеспечения безопасности информации. К мерам защиты относят разработку административных руководящих документов, установку аппаратных устройств или дополнительных программ, основной целью которых является предотвращение преступлений и злоупотреблений [1]. Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно разделить на четыре уровня:

– законодательный: законы, нормативные акты, стандарты и т. п.;

– административный: действия общего характера, предпринимаемые руководством организации;

– процедурный: конкретные меры безопасности, имеющие дело с людьми;

– программно-технический: конкретные технические меры.

Рассмотрим некоторые меры защиты информационной безопасности компьютерных систем.

Аутентификация пользователей. Данная мера требует, чтобы пользователи выполняли процедуры входа в компьютер, используя это как средство для идентификации в начале работы. Для аутентификации личности каждого пользователя нужно использовать уникальные пароли, не являющиеся комбинациями личных данных пользователей, для пользователя. Необходимо внедрить меры защиты при администрировании паролей, и ознакомить пользователей с наиболее общими ошибками, позволяющими совершиться компьютерному преступлению. Если в компьютере имеется встроенный стандартный пароль, его нужно обязательно изменить [2].

Процедуры авторизации. В организации, имеющей дело с критическими данными, должны быть разработаны и внедрены процедуры авторизации, которые определяют, кто из пользователей должен иметь доступ к той или иной информации и приложениям. В организации должен быть установлен такой порядок, при котором для использования компьютерных ресурсов, получения разрешения доступа к информации и приложениям, и получения пароля требуется разрешение тех или иных начальников. Если информация обрабатывается на большом вычислительном центре, то необходимо контролировать физический доступ к вычислительной технике. Могут оказаться уместными такие методы, как журналы, замки и пропуска, а также охрана. Ответственный за информационную безопасность должен знать, кто имеет право доступа в помещения с компьютерным оборудованием и выгонять оттуда посторонних лиц.

Защита носителей информации (исходных документов, лент, картриджей, дисков, распечаток).

Защита данных от перехвата [3]. Для любой из трех основных технологий передачи информации существует технология перехвата: для кабельных линий - подключение к кабелю, для спутниковой связи – использование антенны приема сигнала со спутника, для радиоволн - радиоперехват. Российские службы безопасности разделяют коммуникации на три класса. Первый охватывает локальные сети, расположенные в зоне безопасности, т. е. территории с ограниченным доступом и заэкранированным электронным оборудованием и коммуникационными линиями, и не имеющие выходов в каналы связи за ее пределами. Ко второму классу относятся каналы связи вне зоны безопасности, защищенные организационно-техническими мерами, а к третьему - незащищенные каналы связи общего пользования. Применение коммуникаций уже второго класса значительно снижает вероятность перехвата данных.

Для защиты информации во внешнем канале связи используются следующие устройства: скремблеры для защиты речевой информации, шифраторы для широковещательной связи и криптографические средства, обеспечивающие шифрование цифровых данных.

Заключение. В результате были рассмотрены основные компьютерные преступления, способы защиты информации от несанкционированного доступа. Также рассмотрены меры безопасности информационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Защита информации [Электронный ресурс]. Общие сведения об угрозах безопасности – Режим доступа: http://sosh11.edusluda.ru/index.php/uchenikam/uchebnye-materialy/informatika-i-ikt/103-11-klass/89-zashchita-informatsii-ot-nesanktsionirovannogo-dostupa, свободный. – Загл. с экрана. – Яз. Рус.
2. Методы и способы защиты информации от несанкционированного доступа [Электронный ресурс] Консультант Плюс http://www.consultant.ru, свободный. – Загл. с экрана. – Яз. Рус.
3. Агеев С.А., Бушуев А.С., Егоров Ю.П., Саенко И.Б. Концепция автоматизации управления информационной безопасностью в защищенных мультисервисных сетях специального назначения // Автоматизация процессов управления. 2011. № 1. С. 50-57

УДК 004.056.53

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА ОСНОВЕ ВЫБОРА ЗАЩИЩЕННЫХ ИНТЕРВАЛОВ СВЯЗИ ОТ РАДИОПОДАВЛЕНИЯ

Митрофанов Михаил Валерьевич., Ракицкий Станислав Николаевич, Чиков Дмитрий Викторович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: dmitry-chikov@yandex.ru

Аннотация. В докладе рассмотрен подход повышения помехозащищённости систем управления и связи. Предлагается подход к обоснованию выбора, защищённого от радиоподавления интервала связи, на основе выбора защищённого интервала связи от радиоподавления.

Ключевые слова: *помехозащищённость; радиоподавление.*

SECURITY OF TELECOMMUNICATION NETWORKS BASED ON THE SELECTION OF PROTECTED INTERVALS WHEN JAMMING

Mitrofanov Michael, Rakitskiy Stanislav, Chikov Dmitry
Military Academy of communications
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: dmitry-chikov@yandex.ru

Abstract. The article considers the problem of increasing noise immunity of the systems of control and communication. The approach to substantiation of a choice that is protected from jamming interval when, based on the selection of protected interval communications from jamming.

Keywords: *noise immunity; radio countermeasure.*

В связи с усложнившейся военно-политической обстановкой в мире, задача повышения помехозащищенности систем управления и связи является весьма острой и до сих пор не нашла своего решения в большинстве прикладных задач [1]. Решению этой задачи способствует комплексное использование различных методов и средств (сигналов сложной формы, оптимальных методов их обработки, фазированных антенных решеток, быстродействующей цифровой техники, современной технологии, организационных мер). Однако применение этих способов не обеспечивает выполнение требований по помехозащищенности при постановке противником заградительных помех [2].

Таким образом, возникло противоречие между развитием способов воздействия противника на радио электронные средства (РЭС) и устаревшими подходами к обеспечению и оценки помехозащищенности РЭС.

С целью устранения указанного противоречия предлагается подход к обоснованию выбора, защищённого от радиоподавления интервала связи [3].

Вероятность радиоподавления зависит от:

– вероятности частотно-временного контакта излучения преднамеренной помехи с приемником сигнала;

– вероятности принятия решения на подавление;

– вероятности доставки забрасываемых передатчиков помех (ЗПП) к объекту подавления.

Исходя из условий задачи, примем что вероятность радиоподавления и вероятность доставки ЗПП к объекту подавления равны единицы, задавшись допустимым значением вероятности принятия решения равным 0,15.

Значение вероятности частотно-временного контакта излучения преднамеренной помехи с приемником сигнала определяется по методике, изложенной в [4]. По графику (таблице) табулированной функции Лапласа для трассы радио подавления (РП) определяется допустимое значение аргумента U. С помощью U рассчитываем среднее превышение уровня сигнала над уровнем помех на входе приемника, при котором среднее превышение уровня сигнала над уровнем помех на входе приёмника равно сумме среднеквадратичного отклонения превышения уровня сигнала над уровнем помех и значения величины среднего превышения уровня сигнала над уровнем помех на входе приемника.

На реальных трассах РП величина значения среднего превышения уровня сигнала над уровнем помех на входе приемника определяется из соотношения уровня сигнала над уровнем помех на входе приемника [4].

Значение уровня сигнала и уровня помех на входе приемника определяется с помощью первого уравнения передачи, где суммарный множитель ослабления сигнала (помехи) на интервале связи, определяется протяженностью интервала связи и рабочей частотой. Приняв, что коэффициент полезного действия фидеров антенных устройств средств связи и станций РП равны между собой, входы передающих антенн и выходы передатчиков, а также выходы приемных антенн и входы приемников полностью согласованы по сопротивлению, и все антенны согласованы по поляризации, получим выражение, удобное для расчета дальности связи.

По графику нормального распределения функции Лапласа находим параметр распределения функции Лапласа.

Анализ результатов, полученных с помощью приведенного подхода показывает, что протяжённость защищённого от радиоподавления интервала связи зависит от дальности, на которой ведётся подавление.

Данный подход обеспечения безопасности телекоммуникационных сетей позволяет обосновать защищенный интервал связи от преднамеренных помех.

СПИСОК ЛИТЕРАТУРЫ

1. Лепешкин О.М. Исследование функциональной безопасности систем государственного управления. Инфокоммуникационные технологии. 2007. Т.5. №3. С.165-166.
2. Лепешкин О.М., Корсунский А.С. Оптимизация структуры комплекса информационно-технических средств в автоматизированных системах управления. Автоматизация процессов управления. 2011. №4. С.76-81.
3. Комарович В.Ф., Симонов М.В., Фролов В.Ю. Основы радиоэлектронной борьбы, радиоэлектронная защита и безопасность связи и АСУ. Инв. № 77420. – Л.: ВАС, 1989. – 346 с.
4. Антонюк Л.Я., Игнатов В.В. Эффективность радиосвязи и методы её оценки. – СПб.: ВАС, 1994. – 138 с.

УДК 654.165

ИССЛЕДОВАНИЕ ПРОЕКТИРОВАНИЯ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ

Михайлов Вячеслав Викторович[1], Ильичёв Святослав Игоревич[1], Федосеев Денис Олегович[1], Степанова Елена Александровна[2]

[1]Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3

[2]ФГБУ «16 Центральный научно-исследовательский испытательный институт» Министерства обороны Российской Федерации
Россия, Московская обл., Мытищи, ул. Комарова, 17
e-mails: kycha-mala@mail.ru, svyatoslav_cv@mail.ru

Аннотация. Рассматривается технология и основные средства проектирования программно-конфигурируемых сетей на основе протокола OpenFlow. Стремительное развитие вычислительной производительности, объемов памяти и возможностей высокоскоростной передачи данных привело к необходимости разработки новых технологий построения сетевых инфраструктур.

Ключевые слова: *передача данных; защита информации; сети; Интернет.*

RESEARCH OF DESIGNING PROGRAM-CONFIGURABLE NETWORKS

Mikhailov Vyacheslav[1], Il'ichev Svyatoslav[1], Fedoseev Denis[1], Stepanova Elena[2]

[1]S.M. Budjonny Military Academy of the Signal Corps,
Russia, St. Petersburg, Tikhoretsky st. 3,

[2]FGBU «16 Central research test Institute» of the Ministry of defence of the Russian Federation
Russia, Russia, Moscow region, Mytischi, Komarovastr., 17
e-mails: kycha-mala@mail.ru, svyatoslav_cv@mail.ru

Abstract. Discusses the technology and basic design tools software defined networking based on OpenFlow Protocol. The rapid development of computing power, memory and capabilities of high-speed data transmission has led to the development of new technologies of constructing network infrastructures.

Keywords: *data transmission; protection of information; networks; Internet.*

В обычном маршрутизаторе Internet одновременно реализуются и управление, и передача данных.

Уровень управления представлен встроенным контроллером, уровень передачи данных – таблицей коммутации и коммутационной матрицей. Контроллер обладает интеллектуальными функциями, позволяющими ему самому принимать решения о передаче данных на основе информации о структуре сети. Но непосредственно управлять принятием решения нельзя – можно лишь конфигурировать контроллер, задавая определенные наборы правил и приоритетов.

Это значительно ограничивает функциональность коммутатора и всей сети. Проблему разделения уровня управления и передачей данных исследователи Стэнфорда и Беркли предложили решить в рамках подхода, получившего название программно-конфигурируемые сети (ПКС).

Программно-конфигурируемые сети (Software Defined Networks, SDN) – развивающаяся архитектура сети, где функция управления сетью разделена с функцией передачи данных и полностью программируема [1].

Основная идея ПКС состоит в том, чтобы, не изменяя существующего сетевого оборудования отделить управление этим оборудованием (маршрутизаторами и коммутаторами) за счет создания специального программного обеспечения, которое может работать на обычном отдельном компьютере и находится под контролем администратора сети.

Теоретически ПКС дает возможность абсолютной гибкости в управлении трафиком, а также обеспечивает легкую балансировку трафика без задействования отдельного специализированного оборудования. Самым используемым протоколом для поддержания обмена между контроллерами и коммутаторами ПКС является протокол OpenFlow.

Для проектирования и анализа инфраструктуры программноконфигурируемых сетей с поддержкой протокола OpenFlow наиболее часто используют эмулятор MiniNet. Он моделирует компьютерные сети, создавая виртуальные узлы, коммутаторы, контроллеры и каналы связи. Следовательно, топологии, построенные и работающие в MiniNet, могут быть применимы в реальных сетях, состоящих из реальных аппаратных устройств.

MiniNet предоставляет пользователям готовые решения для получения сведений о поведении и производительности ПКС архитектур, реализованных на различных экспериментальных сетевых топологиях. Появляется возможность комплексного тестирования сложных топологий без запуска физической сети. Эмулятор поддерживает не только базовый набор встроенных топологий, но и произвольные пользовательские топологии. Их создание возможно с помощью сценариев, написанных на языке Python. Так же для программирования контроллеров OpenFlow сетей используют язык Frenetic [2].

Это новый, объектно-ориентированный язык, встроенный в Python, который включает в себя:

1) ограниченный, но высокоуровневый и декларативный язык сетевых запросов,

2) функциональную библиотеку политик управления сети. Frenetic предоставляет программисту интерфейс для классификации сетевого трафика, а также набор правил фильтрации, группировки и передачи пакетов. Объединяя возможности Python и Frenetic, был создан язык Pyretic [3,4].

Pyretic одновременно является объектноориентированным языком программирования, встроенным в Python, и системой исполнения, которая реализует программы, написанные на языке Python на сетевых коммутаторах. Он позволяет сетевым программистам и операторам создавать емкие модульные сетевые приложения, предоставляя им мощные абстракции. За счет этого основное внимание уделяется способу задания сетевых политик. Например, с использованием Pyretic программисты могут задать правила передачи трафика в виде компактных абстрактных функций, которые на входе получают пакет, а на выходе возвращают набор новых пакетов.

Pyretic облегчает модульное проектирование за счет использования двух правил взаимодействия операторов: параллельного и последовательного, позволяющих программистам комбинировать множество правил без опасения возникновения конфликта между ними.

Разработчики приложений так же могут создавать динамические правила, которые меняют свое поведение в течение времени [5]. Таким образом, Pyretic предоставляет ПКС-программистам краткий модуль сетевого приложения как абстракцию высокого уровня.

СПИСОКЛИТЕРАТУРЫ

1. «Software-defined networking: the new norm for Networks», ONF White Paper. April 2012.
2. N. Foster, M. J. Freedman et al, «Languages for software-defined networks», IEEE Communications Magazine. 2013. Vol. 51, Issue 2. pp. 128-134.
3. J. Reich, C. Monsanto et al, «Modular SDN Programming with Pyretic», USENIX;login: Magazine. Vol. 38, Issue 5. 2013. pp.128-134.
4. Брунилин А.А., Бирюков М.А., Саенко И.Б. Модель и метод использования онтологий для управления разграничением доступа в едином информационном пространстве // Математические методы в технике и технологиях – ММТТ. 2016. № 6 (88). С. 122-124.
5. Агеев С.А., Шерстюк Ю.М., Саенко И.Б., Полубелова О.В. Концептуальные основы автоматизации управления защищенными мультисервисными сетями // Проблемы информационной безопасности. Компьютерные системы. 2011. № 3 С. 30-39.

УДК621.391(075.8)

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Михайличенко Николай Валерьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: 23esn2008@rambler.ru

Аннотация. Вопросы защиты данных в настоящее время являются критическими при обеспечении безопасности современных центров обработки данных. Настоящая работа посвящена рассмотрению ситуации, которая сложилась в области безопасности данных, находящихся в центрах обработки данных. Сформулированы перспективные пути исследований и развития систем защиты информации центров обработки данных.

Ключевые слова: *центр обработки данных; система управления; информационная безопасность.*

PROBLEMS AND PROSPECTS OF DATA CENTERS SECURITY

Mikhaylichenko Nikolay
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail:23esn2008@rambler.ru

Abstract. Questions of data protection are critical at safety of modern data-processing centers now. The real work is devoted to consideration of a situation, which has developed in the field of data security, being in data-processing centers. Perspective ways of researches and development of systems of information security of data-processing centers, are formulated.

Keywords: *control system; data center; information security.*

Несмотря на постоянные сообщения о "хакерских атаках", наносящих убытки, все больше и больше компаний для организации своего бизнеса использует Интернет. Хорошо это или плохо сказать тяжело, но это неизбежно. Сегодня Интернет - единственное действительно всеобщее пространство, позволяющее, хранить, передавать, обрабатывать информацию, имеющее развитую мировую инфраструктуру.

В связи с этим все большее распространение получают услуги современных центров обработки данных (ЦОД), которые обеспечивают надежный хостинг и предусматривают расширенные возможности обеспечения безопасности данных. Так, например, при удаленной работе с приложениями по схеме ASP (аренда приложений, Application Service Provision) безопасность обеспечивается за счет комплексной системы защиты, включающей в себя сканеры обнаружения вторжений, межсетевые экраны, системы аудита журнальных файлов, системы анализа статистических характеристик трафика.

Задачи информационной безопасности ЦОД сводятся к минимизации ущерба при возможных воздействиях, а также к предсказанию и предотвращению таких воздействий.

Соответственно, составляющими информационной безопасности ЦОД являются: определение объектов, на которые могут быть направлены угрозы, выявление существующих и возможных угроз, определение возможных источников угрозы, оценка рисков, методы и средства обнаружения враждебного воздействия, методы и средства защиты от известных угроз, методы и средства реагирования при инцидентах. Рассмотрим ряд элементов ЦОД которые могут быть подвержены нарушению безопасности [1].

Оборудование и элементы инфраструктуры ЦОД к ним относятся серверы, активное сетевое оборудование, кабельные системы, электропитание, вспомогательные системы. Для таких объектов существует угроза физического воздействия, которое может привести к повреждению объекта, потере функциональности, либо к появлению в системе чужеродных объектов, влияющих на работу системы или осуществляющих съем информации.

Кроме того, существует риск похищения объектов защиты. Для минимизации риска в этом направлении используются классические методы физической защиты (защитный периметр, пропускная система и контроль доступа персонала, видеонаблюдение, системы сигнализации, срабатывающие при похищении оборудования, вооруженная охрана, служба собственной безопасности).

Программное обеспечение систем хранения данных (СХД). Это операционные системы, прикладные программы, сервисы. И это основные цели практически всех классических атак и основные источники уязвимостей ЦОД. Атаки на СХД могу привести: а) к краху системы (программы, сервиса), частичной или полной остановке функционирования ЦОД; б) выполнению атакующей

стороной (или в результате внешнего воздействия) несанкционированных действий внутри системы; в) получению контроля над системой.

Защита от атак, использующих уязвимость программного обеспечения СХД, как правило, и является основной задачей классических систем информационной безопасности.

Персонал, обслуживающий ЦОД. Администратор любого крупного ЦОД должен являться объектом защиты. И объектом пристального внимания службы собственной безопасности. Целенаправленное или случайное воздействие на обслуживающий ЦОД персонал, имеющий административные полномочия в системе, может привести к возникновению существенных рисков. Отмечу также, что для отдельных систем "цена вопроса" может оказаться сопоставимой со стоимостью всей системы.

Рассмотрим некоторые конкретные элементы защиты, их возможные реализации и целесообразность применения в различных ситуациях [2].

"Нулевой" рубеж обороны - это сокрытие структуры сети, так называемая имитационная защита. Специальное программное обеспечение эмулирует сетевые сегменты, сервера и уязвимости. Постоянный контроль за атаками на несуществующую сеть позволяет выявить источники угроз. С другой стороны, имитационная защита вводит в заблуждение потенциальных агрессоров и затрудняет определение истинной структуры системы при планировании атак.

Первый рубеж защиты - детектор вторжений. Производя анализ входящего трафика, эта система отслеживает появление сигнатур известных типов атак. В ряде случаев устанавливается система адаптивной защиты, в которой при обнаружении определенных сигнатур осуществляется изменение списков доступа на сетевом экране (firewall). Таким образом, осуществляется оперативное блокирование источника атаки.

Второй рубеж - разделение зон безопасности, закрытых сетевыми экранами, и разделение трафика за счет использования виртуальных сетей VLAN. Виртуальные сети (VLAN) в классическом хостинге используются значительно реже - в основном из-за другой структуры сети и упоре на виртуальный хостинг. Настройка межсетевых экранов при сложной структуре сети является нетривиальной задачей, и в целом, используется принцип "запрещено все, что не разрешено"[3].

Из других методов защиты, использование которых неизбежно, следует выделить антивирусную защиту. Идеальным решением является централизованный антивирусный мониторинг, причем выбор программного обеспечения здесь достаточно широк.

Контроль доступа и идентификация пользователей – также является неотъемлемой частью системы безопасности. Постоянной проблемой является частая генерация и смена паролей супер-пользователей.

Из соображений безопасности их следует менять действительно часто. Что-либо не происходит, либо пароли root оказываются записанными на всех доступных поверхностях. Неплохим выходом является использование современных средств идентификации и контроля доступа. Собственно, реально используется несколько основных методов, в частности, на основе бесконтактных элементов памяти ("таблеток" Dallas Semiconductor), на основе смарт-карт (Schlumberger), а также системы биометрического контроля.

Помимо этого, производители систем контроля доступа постепенно приходят к удешевлению продуктов, чтобы сделать их более доступными, а также к упрощению их монтажа и эксплуатации. Из последних физических разработок можно выделить биометрические датчики нового типа, идентифицирующие сотрудника по рисунку кровеносных сосудов на пальцах.

Последние, для случая с ЦОД, кажутся предпочтительней, так как палец или глаз потерять сложнее, чем брелок с элементом памяти. И есть гарантия, что в систему входит именно уполномоченный пользователь, а не некто, нашедший ключ.

Таким образом, для обеспечения нормальной работы, в современных ЦОД должны разрабатываться комплексные решения для обеспечения как информационной, так и физической безопасности которые приведут к комплексной защите информации в ЦОД.

СПИСОК ЛИТЕРАТУРЫ

1. Чуднов А.М., Кирик Д.И., Курашев З.В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений / Радиотехнические и телекоммуникационные системы. - 2017. -№2. С.41-49.
2. Саенко И.Б., Бирюков М.А., Ефимов В.В., Ясинский С.А. Модель администрирования схем разграничения доступа в облачных инфраструктурах // Информация и космос. 2017. № 1. С. 121-126.
3. Неижмак А.В., Орешина М.А. Методы защиты облачных хранилищ // Образование и информационная культура: теория и практика. Материалы Межрегионального форума. Под редакцией В.Г. Шубовича. 2016. С.88-92
1. Неижмак А.В., Тихонов Д.О. Назначение и основные характеристики систем повышения достоверности в каналах и сетях передачи данных специального назначения и пути их решения// Образование и информационная культура: теория и практика. Сборник научных трудов. 2017. С. 46-49

УДК621.391(075.8)

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МОБИЛЬНЫХ УСТРОЙСТВАХ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ

Неижмак Алексей Владимирович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: leshechka_87@mail.ru

Аннотация. Рассмотрены некоторые способы хищения персональных данных из мобильных устройств и несколько вариантов их предотвращения. Описаны наиболее распространенные причины хищений, виды информации, которая чаще всего подвержена атакам, а также неумышленные ошибки пользователей, приводящие к утечкам персональных данных.

Ключевые слова: *мобильные устройства; хищения персональных данных; кибератаки; маскировка; способы защиты устройств.*

PROBLEMS OF INFORMATION SECURITY IN MOBILE DEVICES AND POSSIBLE WAYS OF THEIR SOLUTIONS

Neizhmak Alexey
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: leshechka_87@mail.ru

Abstract. In the article some methods of stealing personal data from mobile devices and several variants of their prevention are considered. The most common causes of theft, types of information most often susceptible to attacks, as well as unintentional errors of users, leading to leaks of personal data are described.

Keywords: mobile devices; theft of personal data; cyberattacks; disguise; ways to protect devices.

Мобильные устройства, под ними мы привыкли понимать телефоны и смартфоны, являются сегментом, которому уделяется особое внимание благодаря удобному и выгодному развитию всевозможных технологий и сервисов в данной отрасли. И чем большее развитие получает направление мобильных устройств, тем острее встаёт вопрос об обеспечении безопасности владельца устройства и его персональных данных.

Опасность хищения персональных данных возрастает пропорционально расширению функционала мобильных устройств, который напрямую связан с аппаратной и программной составляющей. Мобильное устройство способно выступать в качестве привычного каждому настольного компьютера. Если посмотреть на программную составляющую, то, для начала, стоит отметить популярные мобильные платформы – это Android, IOS, Windows. Для Android и IOS, можно выделить, огромное множество программных продуктов и всевозможных сервисов, которые могут удовлетворить практически все потребности требовательных пользователей. Развитие мобильных устройств в настоящее время находится на высоком уровне, следовательно, данному уровню должна соответствовать и защита [1].

Каждый пользователь мобильных устройств подвержен риску кибератак. Количество моделей многократно увеличивается, поэтому, как правило, поддержка ранних устройств и ранних версий операционных систем осуществляется недостаточно долго. С выходом свежих версий программного обеспечения мы получаем вместе с обновлённой операционной системой уязвимости и недоработки, которые разработчики стремятся исправить в обновлениях [2].

Часто пользователи страдают от приложений, которые лишены таких изобретательных методов, как описывалось ранее. Владельцам современных гаджетов должны быть знакомы с онлайн-магазинами iTunes Store, Google Play, Windows Phone Store, в которых пользователи могут покупать различный контент, а также его распространять. У каждого есть возможность приобрести аккаунт разработчика, и продавать собственные программные продукты в этих магазинах, контент в которых подвергается проверкам. Если в магазине Apple проверки тщательные и строгие, в магазине Google – чуть проще. Возникают ситуации, когда в продажи просачиваются приложения с вредоносным кодом, который, к примеру, похищает логины и пароли, отправляя их третьим лицам. Во избежание неприятных ситуаций стоит пользоваться «софтом» известных разработчиков, которым вы доверяете (стоит помнить, что каждый желающий может приобрести аккаунт разработчика).

Но кража данных происходит не только преступными методами, случается, что пользователь наделяет разработчиков программного обеспечения правами на их использование. В онлайн-магазине перед загрузкой необходимого приложения всплывает окно с запросом разрешая на исполнение приложением ряда действий, принимая данное соглашение перед установкой пользователь может открыть доступ к своим персональным данным и не только своим [3].

Пересылка какой-либо информации происходит в ходе работы системных приложений и приложений известных разработчиков. Это позиционируется, как сбор данных для «удобства» работы пользователя с устройством. Происходит следующее: программа запоминает поисковые запросы, ваши геоданные, статистику работы с приложениями и прочее – эта информация обрабатывается и на её основе, например, в качестве рекламы, предъявляется информация, которая скорее всего будет интересна или близка пользователю. Но это наталкивает на неприятные мысли и чувство вторжения в личную жизнь. Если взглянуть серьёзнее на проблему сбора подобной статистики и обратиться к исследованиям, то получается, что подозрения оказываются не такими уж и беспочвенными [4].

Ещё одной причиной кражи персональных данных может служить потеря вашего мобильного устройства или возможность бесконтрольного доступа к нему. Например, если ваш смартфон остаётся на продолжительное время без присмотра, заинтересованное лицо получает шанс воспользоваться случаем и похитить личную информацию. Аналогична ситуация с потерей или хищением устройства. К счастью, современные гаджеты имеют средства защиты, которые могут свести на нет извлечение данных из устройства, имея к нему физический доступ, без вашего ведома. К ним можно отнести: пароль – простой и действенный способ защиты (эффективность которого зависит от сложности пароля), графический ключ – последовательное соединение опорных точек на экране (не является серьёзной преградой для наблюдательных людей), распознавание лица – использует фронтальную камеру (на качество работы влияет множество факторов), распознавание голоса – запись звукового файла и сравнение с оригиналом, являющимся ключом, дактилоскопический сканер – надёжный способ защиты устройства (количество оснащённых такой функцией устройств растёт), сканер радужной оболочки глаза – использует фронтальную камеру (впервые использовано на флагманах компании Microsoft в 2015 году) [6]. Такие инструменты защиты снижают риски хищения данных через физический доступ к устройству. Для подобных случаев утраты контроля над гаджетом существуют специальные функции – блокировка устройства через интернет, определения местонахождения, удаления данных с устройства [5].

Заключение.Таким образом, приобретая полезные сервисы и удобные функции, мы жертвуем безопасностью своих личных данных. Современному человеку очень сложно отказаться от использования мобильных устройств, так как это практически равносильно изоляции от информационного пространства, что не соответствует установившимся тенденциям и образу жизни общества. Каналы передачи данных обеспечивают нас возможностью доступа практически к любой информации, но нельзя забывать, что это средства двухстороннего обмена данными, поэтому использовать их нужно, не пренебрегая правилами информационной безопасности [6].

СПИСОК ЛИТЕРАТУРЫ

1. Информационная безопасность: учеб. пособие / В.В. Гафнер. — Ростов н/Д : Феникс, 2010. — 324 с.
2. Чуднов А.М., Кирик Д.И., Курашев З.В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений / Чуднов А.М., Кирик Д.И., Курашев З.В. / Радиотехнические и телекоммуникационные системы. - 2017. -№2. с.41-49
3. Брунилин А.А., Бирюков М.А., Саенко И.Б. Модель и метод использования онтологий для управления разграничением доступа в едином информационном пространстве // Математические методы в технике и технологиях – ММТТ. 2016. №6 (88). С. 122-124
4. Башкирцев А.С., Михайличенко Н.В., Ренсков А.А., Паращук И.Б. Совершенствование объема и номенклатуры множества контролируемых параметров, принадлежащих пространству управления информационными системами и сетями // Успехи современной науки 2017, №1, Т.4, С.46-52
5. Овсянников С.Н., Хмелевской В.П. Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 389-391
6. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. - 372 с.

УДК 003.26 (075.8)

ИССЛЕДОВАНИЕ ПРОБЛЕМЫ ПРОСЛУШИВАНИЯ СЕТЕВОГО ТРАФИКА

Нехань Евгений Николаевич, Гудков Михаил Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: jackmanrus@yandex.ru

Аннотация. Приведены результаты анализа проблемы прослушивания сетевого трафика, сформулированы сущность и содержание соответствующей разновидности сетевой атаки. Предложено направление дальнейших исследований – формулировка требований для предотвращения угрозы перехвата трафика.

Ключевые слова: *защита информации; перехват данных; прослушивания сетевого трафик, подмена траффика.*

INVESTIGATION OF THE PROBLEM OF LISTENING THE NETWORK TRAFFIC

Nehan'Evgeny, Gudkov Mikhail
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: jackmanrus@yandex.ru

Abstract. The results of the analysis of the problem of listening to network traffic are presented, the essence and content of the corresponding version of the network attack are formulated. The direction of further research is proposed - the formulation of requirements to prevent the threat of interception of traffic.

Keywords: *data protection; Interception of data; listening to network traffic; spoofing.*

ARP - spoofing (ARP - poisoning) - разновидностьсетевойатакитипа MITM (Man in the middle), применяемаявсетяхсиспользованиемпротокола ARP [1]. В основном применяется в сетях Ethernet. Атака основана на недостатках протокола ARP.

При использовании в распределённой вычислительной сети алгоритмов удалённого поиска существует возможность осуществления в такой сети типовой удалённой атаки «ложный объект распределённой вычислительной системы». Анализ безопасности протокола ARP показывает, что, перехватив на атакующем узле внутри данного сегмента сети широковещательный ARP-запрос, можно послать ложный ARP-ответ, в котором объявить себя искомым узлом (например, маршрутизатором), и в дальнейшем активно контролировать сетевой трафик дезинформированного узла, воздействуя на него по схеме «ложный объект РВС» [2].

ARP - spoofing позволяет злоумышленнику перехватывать кадры данных в сети, изменять трафик или останавливать весь трафик. Часто атака используется как средство для других атак, таких как отказ в обслуживании, MITM или атаки на перехват сеанса. Рассмотрим программу анти-«ARP-спуфинга» shARP, основная функция которой обнаруживать присутствие третьей стороны в частной сети.

Программа shARP имеет 2 режима: оборонительный и наступательный.

Оборонительный режим: защищает конечного пользователя от «спуфинга», отключая систему пользователя от сети и предупреждая пользователя сообщением.

Наступательный режим: отключает систему пользователя от сети, а затем вышвыривает злоумышленника, отправив в его систему пакеты деаутентификации, неспособные к повторному подключению к сети, пока программа не будет перезапущена вручную.

Программа создает файл журнала (/ usr / shARP /), содержащий детали атаки, такие как адрес MAC злоумышленников, время и дату выпуска MAC. С помощью полученного MAC-адреса мы можем идентифицировать сетевую карту системы нападавших. Если требуется, злоумышленник может быть навсегда заблокирован из сети путем подачи его адреса MAC в список блокировки маршрутизатора.

Когда пользователь запускает программу в защитном режиме, как только программа обнаруживает «спуфер» в сети, она отключает систему пользователя от сети, чтобы защитить личные данные, передаваемые между системой и сервером [3]. Она также сохраняет файл журнала о злоумышленнике для дальнейшего использования. На атакующее устройство инициируется атака MITM. Результатом атаки станет то, что атакуемый хост будет отключен от сети.

Заключение. Для уменьшения риска перехвата конфиденциальных данных необходимо следующее:

- использование разных сложных паролей для аутентификации;
- установка и настройка программных или аппаратных средств, распознающих спуфинг;
- использование крипто-шифрования каналов связи
- использование программ для защиты беспроводных сетей.

Наиболее эффективным средством защиты от атак с использованием протокола ARP является функция коммутатора Dynamic ARP Inspection[3].

Dynamic ARP Inspection (Protection) регулирует только сообщения протокола ARP и не может повлиять напрямую на трафик пользователей или другие протоколы[4].

В коммутаторах Cisco функция называется Dynamic ARP Inspection, а в коммутаторах ProCurve - Dynamic ARP Protection. Далее, в описании функции будет использоваться термин Dynamic ARP Inspection, а в соответствующем разделе по настройке функции на коммутаторах ProCurve - Dynamic ARP Protection.

Dynamic ARP Inspection позволяет:

- защитить клиентов в сети от атак с использованием протокола ARP;
- регулировать какие сообщения протокола ARP отбрасывать, какие перенаправлять.

Для правильной работы Dynamic ARP Inspection, необходимо указать какие порты коммутатора будут доверенными, а какие - ненадёжными:

Ненадёжные - порты, к которым подключены клиенты. Для ненадёжных портов выполняется ряд проверок сообщений ARP.

Доверенные - порты коммутатора, к которым подключен другой коммутатор. Сообщения протокола ARP полученные с доверенных портов не отбрасываются.

Принципы работы Dynamic ARP Inspection следующий если порт ненадёжный:

– коммутатор перехватывает все ARP-запросы и ARP-ответы на ненадёжных портах прежде чем перенаправлять их;

– коммутатор проверяет соответствие MAC-адреса IP-адресу на ненадёжных портах.

Проверка соответствия MAC-адреса IP-адресу может выполняться на основании информации:

– базы данных привязки DHCP;

– статических записей.

СПИСОК ЛИТЕРАТУРЫ

1. Jian Guo; San Ling; Huaxiong Wang and Christian Rechberge. Advanced Meet-in-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2 -Nanyang Technological University, Singapore, 2015. – 20c;
2. Фороузан Б. Криптография и безопасность сетей - Москва.: Национальный Открытый Университет "ИНТУИТ" ,2016.
3. Switch and VLAN Security - Aaron Balchunas, 2016;
4. Баранов В.В., Бирюков М.А., Кравченко С.А., Максимов А.С., Саенко И.Б. Имитационная модель для анализа рисков информационной безопасности при проектировании ролевых схем разграничения доступа к базам данных // Актуальные проблемы обеспечения информационной безопасности. Труды межвузовской научно-практической конференции. 2017. С. 26-31

УДК 621.391(075.8)

К ВОПРОСУ ФУНКЦИОНАЛЬНОГО, ОРГАНИЗАЦИОННОГО И СТРУКТУРНОГО ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ВЗАИМОДЕЙСТВИИ РЕГИОНАЛЬНЫХ КОРПОРАТИВНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ С СЕТЬЮ ОБЩЕГО ПОЛЬЗОВАНИЯ

Нехань Евгений Николаевич[1], Паращук Игорь Борисович[2], Скрябин Евгений Андреевич[1]
[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mails: shchuk@rambler.ru, sKryabin.eu@yandex.ru

Аннотация. Приведены результаты анализа элементов организационной и физической структур систем защиты информации при взаимодействии региональных телекоммуникационных сетей с сетью общего пользования, сформулированы сущность и содержание видов обеспечения соответствующих систем защиты. Предложено направление дальнейших исследований – формулировка основных оперативно-технических требований, которые должны быть предъявлены к процессу функционирования современных комплексных систем защиты с учетом все возрастающего перечня угроз, исходящих от сети Интернет.

Ключевые слова: *защита информации; структура; функции; телекоммуникационная сеть; система; данные.*

TO THE QUESTION OF FUNCTIONAL, ORGANIZATIONAL AND STRUCTURAL CONSTRUCTION OF THE INFORMATION SECURITY SYSTEM UNDER INTERACTION OF REGIONAL CORPORATE TELECOMMUNICATION NETWORKS WITH A COMMON USE NETWORK

Nyagan Evgeny[1], Parashchuk Igor[2], Skryabin Evgeny[1]
[1]Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
[2] St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
e-mails: shchuk@rambler.ru, sKryabin.eu@yandex.ru

Abstract. The results of the analysis of the elements of the organizational and physical structures of information security systems in the interaction of regional telecommunications networks with the public network are presented, and the essence and content of the types of provision of appropriate protection systems are formulated. The direction of further research is proposed - the formulation of the basic operational and technical requirements that must be presented for the operation of modern integrated protection systems, taking into account an ever increasing list of threats emanating from the Internet.

Keywords: *data protection; structure; functions; telecommunication network; system; data.*

Рассмотрим основные вопросы архитектурного построения систем защиты информации (СЗИ), которые является функциональной подсистемой соответствующих региональных корпоративных телекоммуникационных сетей (РКТС), поэтому их архитектура будет аналогичной архитектуре РКТС и будет представлять собой функциональное, организационное и структурное построение СЗИ при взаимодействии региональных корпоративных телекоммуникационных сетей с сетью общего пользования (глобальной сетью Интернет).

При этом функциональным построением любой системы называется организованная совокупность тех функций, для регулярного осуществления которых она создается. Тогда функциональное построение СЗИ при взаимодействии РКТС с глобальной сетью Интернет можно интерпретировать как организованную совокупность функций, реализуемых СЗИ.

Под организационным построением СЗИ при взаимодействии РКТС с глобальной сетью Интернет понимается общая ее организация, адекватно отражающая концептуальные подходы к ее созданию. В соответствии с концепцией защиты информации в современных телекоммуникационных сетях, организационное построение СЗИ может быть представлено как организационная система, состоящая из трех частей: механизмов обеспечения защиты информации, механизмов управления механизмами защиты и механизмов общей организации работы системы.

В механизмах обеспечения защиты выделяются два организационных компонента: постоянные (или встроенные) механизмы; переменные (или включаемые-выключаемые) механизмы. При этом под постоянными компонентами понимаются такие механизмы, которые встраиваются в элементы РКТС в процессе создания СЗИ и находятся в рабочем состоянии во все время функционирования соответствующих элементов (узлов, линий и т.п.) телекоммуникационной сети. Переменные же механизмы являются автономными, использование их для решения задач защиты информации предполагает предварительное осуществление операций ввода в состав используемых механизмов. Встроенные и переменные механизмы могут иметь в своем составе технические, программные и организационные средства обеспечения защиты. Соответственно составу механизмов обеспечения защиты информации, очевидно, должны быть организованы механизмы управления ими.

Механизмы общей организации работы СЗИ при взаимодействии РКТС с сетью общего пользования, как следует из самого названия, предназначены для системной увязки и координации работы всех компонентов СЗИ. В понятие организационного построения СЗИ при взаимодействии РКТС с сетью общего пользования входит также распределение элементов этой системы по организационно-структурным элементам РКТС. Исходя из этого, в организационном построении СЗИ должны быть предусмотрены подсистемы защиты на объектах (структурных компонентах) РКТС и некоторое управляющее звено, которое в специальных работах получило название ядра СЗИ [1, 2].

Ядро системы защиты есть специальный компонент системы, предназначенный для объединения всех подсистем СЗИ в целостную единую систему защиты, организации, обеспечения и контроля ее функционирования. Функции ядра СЗИ и способы выполнения этих функций достаточно подробно описаны в [3].

Вопрос о структурном построении СЗИ при взаимодействии РКТС с сетью общего пользования требует особого пристального рассмотрения. Поскольку, как уже отмечалось выше, СЗИ является автоматизированной системой, ее структурное построение может быть определено по аналогии со структурным построением РКТС.

При этом содержание структурных компонентов СЗИ при взаимодействии РКТС с сетью общего пользования в общем виде может быть представлено следующим образом. Человеческий компонент составляют те лица (или группы лиц, коллективы, подразделения), которые имеют непосредственное отношение к защите информации в процессе функционирования РКТС. К ним должны быть отнесены: пользователи РКТС, имеющие доступ к ее ресурсам и участвующие в обработке информации; администрация РКТС, обеспечивающая общую организацию функционирования системы обработки в сети, в том числе и СЗИ; диспетчеры и операторы РКТС, осуществляющие прием информации, подготовку ее к обработке, управление средствами связи и вычислительной техники в процессе обработки, контроль и распределение результатов обработки, а также некоторые другие процедуры, связанные с циркуляцией информационных потоков; администраторы банков данных, отвечающие за организацию; ведение и использование баз данных РКТС; обслуживающий персонал, обеспечивающий работу технических средств РКТС, в том числе и средств СЗИ; системные программисты, осуществляющие управление программным обеспечением РКТС в рамках службы, специально создаваемой для организации и обеспечения зашиты информации.

Информационно-вычислительные ресурсы системы, необходимые для создания и поддержания функционирования СЗИ, как и любой другой автоматизированной системы, объединяются в техническое, математическое, программное, информационное и лингвистическое обеспечение. Состав и содержание перечисленных видов обеспечения определяются:

– техническое обеспечение – совокупность технических средств, необходимых для технической поддержки решения всех тех задач защиты информации, решение которых может потребоваться в процессе функционирования СЗИ. В техническое обеспечение должны быть включены все технические средства защиты, которые могут оказаться необходимыми в конкретной системе и те технические средства, которые необходимы для решения задач управления механизмами защиты;

– математическое обеспечение – совокупность математических методов, моделей и алгоритмов, необходимых для оценок уровня защищенности информации и решения других задач защиты;

– программное обеспечение – совокупность программ, реализующих программные средства защиты, а также программ, необходимых для решения задач управления механизмами защиты. К ним должны быть отнесены также сервисные и вспомогательные программы СЗИ;

– информационное обеспечение – совокупность систем классификации и кодирования данных о защите информации, массивы данных СЗИ, а также входные и выходные документы СЗИ;

– лингвистическое обеспечение – совокупность языковых средств, необходимых для обеспечения взаимодействия компонентов СЗИ между собой, с компонентами РКТС и с внешней средой.

Заключение. Таким образом, в данном докладе проведен анализ элементов организационной и физической структур СЗИ при взаимодействии РКТС с сетью общего пользования, анализ видов обеспечения СЗИ, что, в конечном итоге, позволяет сформулировать основные оперативно-технических требования, которые должны быть предъявлены к процессу функционирования современных комплексных систем защиты с учетом все возрастающего перечня угроз, исходящих от пользователей сети Интернет.

СПИСОК ЛИТЕРАТУРЫ

1. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / П.Н. Дерявин, О.О. Михальский, Д.И. Правиков и др. – М.: Радио и связь, 2000. – 192 с.;
2. Авраменко В.С. Модели защищенности информации от несанкционированного доступа в многорежимных автоматизированных системах и методы ее контроля в условиях неопределенности угроз. // Информация и космос. 2008. № 2. С. 87-94.
3. Гаценко О.Ю. Защита информации. Основы организационного управления. – СПб.: Изд. дом «Сентябрь», 2001. – 228 с.

УДК 004.056.57

МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНЫХ ВОЗДЕЙСТВИЙ

Нечепуренко Александр Петрович, Суетин Артем Игоревич, Муртазин Ильдар Робертович,
Лаута Олег Сергеевич
Военная академия связи имени Маршала Советского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: vlasenko199@yandex.ru, asuetin5@yandex.ru

Аннотация. В работе рассмотрены атаки на каналы управления роботизированных систем и представлен подход по определению вероятностно – временных характеристик

Ключевые слова: *роботизированная система; канал управления; метод преобразования.*

MODELS OF INTELLECTUAL INFLUENCES

Nechepurenko Aleksandr, Suetin Artem, Murtazin Ildar, Lauta Oleg
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckystr., 3
e-mails: vlasenko199@yandex.ru, asuetin5@yandex.ru

Abstract. In article, the attacks to robotic systems are considered, and approach to definition of their probabilistic and time characteristics is also presented.

Keywords: *robotic system; control path; transformation method.*

Роботизированные системы (РТС) как объект управления представляет собой сложную систему, включающую в себя многозвенную механическую конструкцию с исполнительными пневмо-, гидро- или электроприводами, активно взаимодействующую с окружающей средой и характеризующуюся совокупностью параметров, изменяющихся во времени.

Вместе с тем, непосредственное внедрение РТС приводит к усилению опасности существующих и появлению новых атак противника на подлинность и доступность передаваемой информации, передаваемой по каналам управления (КУ) РТС.

Возможными результатами воздействия атак на РТС являются несанкционированный доступ, блокирование управляющей информации, внедрение ложной информации, нарушение установленных регламентов сбора, обработки и передачи информации, отказы и сбои в работе РТС, а также компрометация передаваемой или получаемой информации. Однако, анализ атак показывает, что наиболее опасными для РТС являются атаки, направленные на перехват канала управления, т.е. интеллектуальные воздействия [1].

Под интеллектуальными воздействиями понимаются целенаправленные, согласованные по месту и времени воздействия, предназначенные для перехвата канала управления системой.

Учитывая вышеизложенное, необходимо разработать способы защиты КУ РТС от интеллектуальных воздействий. Для построения системы защиты предлагается первоначально

построить модели интеллектуальных воздействий, определить их вероятностно-временные характеристики [2] и используя полученные, в качестве исходных данных, обосновать защиту КУ РТС.

Подход, рассматриваемый в работе, предполагает построение аналитических моделей интеллектуальных воздействий (ИВ). Результатом моделирования является функция распределения времени и среднее время реализации ИВ. Для построения аналитической модели ИВ применяется подход, основанный на преобразовании стохастических сетей. Этот подход отличается более высокой точностью и устойчивостью получаемых решений и хорошо зарекомендовал себя для моделирования многошаговых стохастических процессов различной природы.

Первым этапом при моделировании является построение эталонной модели [3]. Эталонная модель атаки – это последовательность (алгоритм) действий злоумышленника при реализации ИВ. В качестве примера построения эталонной модели атаки рассмотрена атака «Человек по середине».

Следующий этап - построение стохастической сети и нахождение эквивалентной функции [4], сохраняющей в своей структуре параметры распределения и логику взаимодействия элементарных случайных процессов. Эквивалентная функция позволяет определить первые моменты случайного времени выполнения целевого процесса.

Далее используя преобразование Лапласа и разложение Хевисайда, находятся расчетные выражения для определения функции распределения вероятности времени реализации ИВ «Человек по середине» и среднее время, затрачиваемое на реализацию ИВ «Человек по середине».

Результаты расчеты представляются в виде зависимостей интегральной функции распределения вероятности от времени реализации ИВ и зависимость среднего времени реализации ИВ от вероятности [5].

Таким образом, предлагается новый подход к аналитическому моделированию атак, основанный на методе преобразования стохастических сетей. Сущность данного метода заключается в замене множества элементарных ветвей стохастической сети одной эквивалентной ветвью и последующим определением эквивалентной функции сети, а также начальных моментов и функции распределения случайного времени реализации атаки.

Проверка предложенного подхода была произведена для моделирования ИВ «Человек по середине», которые являются одними из наиболее распространенных и опасных для компьютерных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Баранов В.В., Гудков М.А., Крибель А.М., Лаута О.С., Нечепуренко А.П. Защита канала управления роботизированных систем. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 32-37.
2. Баранов В.В., Крибель А.М., Лаута О.С., Нечепуренко А.П. Применение метода топологического преобразования стохастических сетей для оценки эффективности средств защиты. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 47-52.
3. Елисеев А.И., Долгов А.А., Хорохорин М.А., Лаута О.С., Набатов К.А. Обеспечение живучести информационных систем (часть 3. Методы обеспечения и повышения живучести). Вестник Воронежского института ФСИН России. 2013. №1. С.91-94.
4. Коцыняк М.А., Лаута О.С., Нечепуренко А.П., Штеренберг И.Г. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия. Труды учебных заведений связи. 2016. Т. 2. № 4. С. 82-87.
5. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 83-89.
6. Карпов А.В., Лепешкин О.М., Попов Н.А. Структура электромагнитного поля при нелинейной радиолокации. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С.1118.

УДК 621.396(075.8)

МОДЕЛИРОВАНИЕ ТЕРРИТОРИАЛЬНОГО РАСПРЕДЕЛЕНИЯ БАЗОВЫХ СТАНЦИЙ СЕТЕЙ ШИРОКОПОЛОСНОГО РАДИОДОСТУПА

Овсянников Станислав Николаевич, Панин Роман Сергеевич, Калюка Владимир Иванович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: stasfvo@mail.ru, zzz822@mail.ru, kvi_spb@rambler.ru

Аннотация. В работе проанализированы вопросы планирования сетей широкополосного радиодоступа. Предложены модели для комплексного расчета оптимальных зон обслуживания и технических характеристик базовых станций при планировании или адаптации радиопокрытия кластера любой размерности и геометрической структуры.

Ключевые слова: *сеть широкополосного радиодоступа; базовая станция; частотно-территориальное планирование; моделирование.*

MODELING OF BROADBAND RADIO ACCESS NETWORKS BASE STATIONS ALLOCATION

Ovsyannikov Stanislav, Panin Roman, Kalyuka Vladimir
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: stasfvo@mail.ru, darius2193@gmail.ru, kvi_spb@rambler.ru

Abstract. The paper analyzes the problems of broadband radio access networks planning. The models for complex calculation of optimal service areas and technical characteristics base stations when planning or adapting for any size and geometric structure of cluster radio coverage are proposed.

Keywords: *wireless subscriber access network, base station, regional frequency planning, modeling.*

Процесс успешной эксплуатации современной сотовой сети подвижной связи зависит не только от первоначального планирования, но и от её адаптации к изменяющимся условиям. В больших городах с развитой инфраструктурой постоянно изменяющаяся обстановка заставляет незамедлительно реагировать на происходящие вокруг изменения. Постоянное увеличение объемов передаваемой информации требует оптимизации сотовой структуры построения сети, поиска оптимальных методов обеспечения электромагнитной совместимости (ЭМС), территориального распределения частотного ресурса, ведения постоянного мониторинга перегрузок с последующим перераспределением ресурса. Высокая эффективность качества работы сети в таких условиях обеспечивается при тесном взаимодействии служб планирования, оптимизации и эксплуатации сети путем использования дорогостоящего программного обеспечения с использованием моделей распространения электромагнитных воли в различных условиях с учетом рельефа местности на основе геоинформационных технологий и контроля ЭМС [1, 2].

В области планирования сети подвижной связи имеются как методики частотно-территориального покрытия, так и прогноза зон обслуживания (радиопокрытия) базовых станций (БС).

Частотно-территориальное планирование состоит из этапов получения исходных данных, калибровки математической модели распространения радиоволн на основе измерений напряженности поля сигнала БС в наиболее характерных точках зоны обслуживания, построения первого приближения зон обслуживания сотовой радиосети, их оптимизации с использованием программного обеспечения, учитывающего эксплуатационные характеристики используемого оборудования [3].

В основе работы сред планирования (программных комплексов), которые широко используются операторами сотовых сетей для составления предварительного плана радиопокрытия, лежат статистические и детерминированные методы [4], которые учитывают параметры, описывающие географический район развертывания сети при прогнозе зон обслуживания БС.

Недостатком существующих сред планирования является их неспособность производить комплексный (одновременный) расчет зон обслуживания БС кластера с учетом их взаиморасположения. Кроме того, при использовании известных сред планирования требуется предварительное, интуитивное задание технических характеристик БС (таких как мощность передатчиков, азимуты антенн, высоты подвеса и др.)

В связи с этим возникает потребность создания простого алгоритма и работающего на его основе программного комплекса первоначального планирования сотовой сети связи на местности с точки зрения охвата радиопокрытием определенной территории кластером различной размерности и структуры (конфигурации).

В процессе эксплуатации сотовой сети возникает необходимость в адаптации (перепланирования) зон обслуживания, например, из-за изменений застройки местности, из-за изменений нагрузки (трафика) БС кластера. Поэтому под задачей адаптации радиопокрытия кластера сотовой сети будем понимать задачу необходимого изменения зон обслуживания группы БС, образующей кластер различной размерности и структуры.

Как в случае планирования, так и в случае адаптации радиопокрытия кластера необходимо добиться оптимального распределения зон обслуживания в кластере.

Однако на практике с учетом рельефа местности и застройки, как правило, невозможно формирование однородного кластера и расположение БС соответствует центрам неравновеликих шестиугольников сот, образующих неоднородный кластер. Для неоднородного кластера мощности излучения БС должны быть разными. При этом необходимо, чтобы зоны недопокрытия, где невозможно облуживание мобильного абонента, отсутствовали. Поэтому для неоднородного кластера термин «оптимальное обслуживание» подразумевает отсутствие зон недопокрытия при минимизации зон перекрытия соседних БС.

Несмотря на схожесть задач планирования и адаптации зон обслуживания БС, методы их решения разные. При планировании расчет зон обслуживания производится поэтапно. Иная ситуация при решении задачи адаптации на уже эксплуатируемой сети. В этом случае изначально имеется кластер из БС, каждая из которых характеризуется расположением относительно соседних своей зоной обслуживания, интенсивностью трафика и его зависимостью от размеров зоны обслуживания.

Изменение какого-либо параметра в кластере, например, уменьшение зоны обслуживания какой-либо БС с целью уменьшения трафика, требует увеличения зон обслуживания соседних БС на высвободившейся территории и, следовательно, увеличение их трафика. В свою очередь перераспределение трафика требует нового цикла расчета оптимальных зон обслуживания БС. Таким образом, очевиден итерационный процесс вычисления зон обслуживания при решении задачи адаптации. Исходными данными в этом случае являются размерность, геометрическая структура кластера и зависящие от реального (статистически измеренного) трафика размеры зон обслуживания каждой БС.

Используя математические модели кластера любой размерности и геометрической структуры, возможен комплексный расчет оптимальных зон обслуживания БС при первоначальном планировании и при адаптации радиопокрытия кластера, необходимость в которой возникает в процессе эксплуатации сотовой сети. В основе предложенных моделей лежит математическое описание кластерной системы, учитывающее взаимное положение БС и величины их трафиков. Математической моделью кластера при планировании радиообслуживания является система линейных алгебраических уравнений, которую можно представить в виде векторно-матричного уравнения с вектором искомых радиусов зон обслуживания БС, вектором известных пролетов между БС и матрицей эластичности с элементами, зависящими от трафика БС. Математической моделью кластера при адаптации радиообслуживания является система нелинейных алгебраических уравнений, которую можно представить в виде векторно-матричного уравнения с вектором искомых радиусов зон обслуживания БС, вектором известных расстояний между БС и матрицей эластичности с элементами, зависящими от радиусов зон обслуживания БС. Предложенные модели обладают вычислительной простотой, требуют минимальный набор начальных данных, пригодных для различных стандартов сотовых сетей связи.

Использование предложенных математических моделей для комплексного расчета оптимальных зон обслуживания и технических характеристик БС при планировании или адаптации радиопокрытия кластера различной размерности и геометрической структуры, имеет существенное значение для экономии интеллектуальных и материальных ресурсов операторов сотовой связи.

СПИСОК ЛИТЕРАТУРЫ

1. Попов В.И. Основы сотовой связи стандарта GSM. - М.: Эко-Трендз, 2005. -296с.: илл.
2. Бабков В.Ю., Вознюк М.А., Михайлов П.А. Сети мобильной связи. Частотно-территориальное планирование. Учебное пособие для вузов // 2-е изд., испр. - М.: Горячая линия - Телеком, 2007. - 224 с.: ил.
3. Шорин О.А., Косинов М.И. Повышение емкости сотовой системы связи при использовании зон перекрытия// «Электросвязь». - № 3, 2003.
4. Бабков В.Ю., Вознюк М.А., Дмитриев В.И. Системы мобильной связи / СПб. СПб ГУТ, 1998.

УДК 621.391(075.8)

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ БЕСПРОВОДНОГО АБОНЕНТСКОГО ДОСТУПА

Овсянников Станислав Николаевич, Панин Роман Сергеевич, Калюка Владимир Иванович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: stasfvo@mail.ru, zzz822@mail.ru, kvi_spb@rambler.ru

Аннотация. Пранализированы вопросы информационной безопасности в сетях беспроводного абонентского доступа. Приведена классификация основных уязвимостей и угроз и рекомендуемые меры по их устранениюв сетях беспроводного абонентского доступа.

Ключевые слова: *сеть беспроводного абонентского доступа; информационная безопасность; протоколы.*

INFORMATION SECURITY PRINCIPLES OF WIRELESS SUBSCRIBER ACCESS NETWORKS

Ovsyannikov Stanislav, Panin Roman, Kalyuka Vladimir
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: stasfvo@mail.ru, zzz822@mail.ru, kvi_spb@rambler.ru

Abstract. The paper analyzes the information security principles of wireless subscriber access networks. A classification of the main vulnerabilities and threats and recommendations for their elimination in wireless subscriber access networks is described.

Keywords: *wireless subscriber access network; information security; protocols.*

Принципиальным отличием технологий беспроводного доступа является использование свободного пространства как ненаправленной среды передачи электромагнитных волн. Основными достоинствами беспроводных технологий являются мобильность, оперативность развертывания, слабая зависимость от местоположения, а недостатком – уязвимость к внешним воздействиям, в том числе и различным видам атак на сети беспроводного абонентского доступа (СБАД) (далее сети).

В качестве управляющей основы типовой беспроводной сети служат ее протоколы, которые регламентируют маршрутизацию, адресацию, топологию сети, порядок доступа узлов к каналу передачи данных, формат передаваемых пакетов, набор управляющих команд и систему защиты информации. Протоколы определяют правила обмена на различных уровнях функциональной архитектуры эталонной модели взаимодействия открытых систем (ЭМВОС).

В зависимости от масштаба (максимального радиуса действия) выделяют несколько типов беспроводных сетей:

– персональная беспроводная сеть (WPAN-Wireless Personal Area Network);
– локальная беспроводная сеть (WLAN-Wireless Local Area Network);
– городскаябеспроводнаясеть (WMAN-Wireless Metropolitan Area Network);
– глобальная беспроводная сеть (WWAN-Wireless Wide Area Network).

Угрозы нарушения информационной безопасности любой телекоммуникационной системы могут быть разделены на три группы:

1. угрозы сообщению, целью которых являются отдельные сообщения, передаваемые пользователями системы, сетевыми операторами и др.;

2. угрозы пользователю, целью которых являются пользователи и их деятельность, как например, контроль над тем, что они делают, где и когда;

3. угрозы системе, целью которых является получение доступа к системе или нарушение ее работы [1].

Информационная безопасность в сети обеспечивается процедурами аутентификации (идентификации, авторизации) и криптозащиты. Средства обеспечения безопасности делятся на две группы: средства шифрации (набор криптографических пакетов) и протоколы управления ключами.

Идентификация – процедура распознавания пользователя по его идентификатору (имени).

Аутентификация – процедура проверки подлинности заявленного пользователя, процесса или устройства.Авторизация – процедура предоставления субъекту определенных полномочий и ресурсов в данной системе [2].

Основные риски и уязвимости для беспроводных протоколов: ключи устройства используются повторно и скомпрометированы; отсутствует аутентификация пользователей; слабые процедуры аутентификации устройств, процессов, пакетов, пользователей; повтор попыток аутентификации; уязвимость для атак во время процесса обнаружения и подключения; перехват беспроводного соединения; перехват информации на узлах сети и при передаче между узлами сети; загрузка программного кода и его исполнения на узлах сети; пассивное прослушивание (eavesdropping); отказ в обслуживании (Denial of Service); захват ресурса (resource misappropriation), атака посредника или атака «человек посередине» (man-in-the-middle attacks); атаки «грубой силы» (brute-force) или полного перебора; ненадежное хранение ключей шифрования; перехват ключа шифрования; использование слабых алгоритмов шифрования.

Для принятия надлежащих мер по защите от вышеперечисленных угроз необходимо принять во внимание:

– виды атак, которые могут быть предприняты для осуществления угроз;
– наличие слабых, с точки зрения информационной безопасности, точек системы (радиоинтерфейс МС (мобильной станции) и БС (базовой станции), проводные интерфейсы, обеспечивающие связь с терминалами, интерфейсы связи с другими сетями, интерфейсы управления сетью и обслуживания сети, другие элементы инфраструктуры транкинговых сетей, такие как базы данных и сетевые узлы и т.п.)
– наличие лиц, которые могут быть заинтересованы в проведении атак (законные пользователи, обслуживающий персонал, сторонние лица);
– специфику и сложность реализации различных видов атак (атаки, которые могут быть проведены практически любым лицом, используя только общедоступную информацию о системе; атаки, для которых требуется оборудование, доступное в свободной продаже; атаки, для выполнения которых требуется оборудование, специально разработанное или существенно модифицированное из имеющегося в наличии) [1].

Таким образом, для защиты передаваемой, хранимой и обрабатываемой информации от существующих угроз при создании СБАД необходимо использовать криптографически стойкие алгоритмы шифрования, максимально использующие свойства сети, топологий, устройств, которые будут устойчивы к различным видам атак, надежные протоколы смены и генерации ключей,

надежные протоколы аутентификации, а также уделять особое внимание возможности использования особенностей случайного и детерминированного сетевого кодирования.

СПИСОК ЛИТЕРАТУРЫ

1. Бабков В.Ю., Цикин И.А. Сотовые системы мобильной радиосвязи: учеб. пособие. 2-е изд., перераб, и доп. – СПб.: БХВ-Петербург, 2013. – 432 с.: ил. – (Учебная литература для вузов).
2. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учеб. пособие. – М.: РИОР; ИНФРА-М, 2013.

УДК: 62-503.57

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ДЕМОДУЛЯЦИИ СИГНАЛОВ

Овчинников Николай Юрьевич, Петренко Михаил Игоревич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: barmaglot12lister@mail.ru

Аннотация. Рассматривается задача демодуляции сигналов. В программном пакете MATLAB разработана модель нейронной сети для определения способа квадратурной амплитудной (QAM-4) демодуляции сигнала.

Ключевые слова: *нейронная сеть; демодуляция сигналов.*

NEURAL NETWORK APPLYING FOR SIGNAL'S DEMODULATION

Petrenko Mikhail, Ovchinnikov Nikolay
S.M. Budjonny Military Academy of the Signal Corps
Russia, St. Petersburg, Prospect Tikhoretsky, 3
e-mail: barmaglot12lister@mail.ru

Abstract. The paper describessignals demodulatingtask. Neural network model has been developed in MATLAB to identify method of QAM-4 signal demodulation.

Keywords: *neural network; signal demodulation.*

Алгоритм квадратурной амплитудной модуляции (QAM, Quadrature Amplitude Modulation) представляет собой разновидность многопозиционной амплитудно-фазовой модуляции. При использовании данного алгоритма передаваемый сигнал кодируется одновременными изменениями амплитуды синфазной (I) и квадратурной (Q) компонент несущего гармонического колебания (fc), которые сдвинуты по фазе друг относительно друга на p/2 радиана.

Результирующий сигнал Z формируется при суммировании этих колебаний. На рисунке 1 представлен принцип формирования результирующего колебания Z путем суммирования вектора квадратурной составляющей Q с вектором синфазной составляющей I. Амплитуда вектора Z определяется соотношением Am, а угол, который этот вектор образует с осью абсцисс, определяется соотношением jm.

Для данного алгоритма существенно, что при модулировании синфазной и квадратурной составляющей несущего колебания используется одно и то же значение дискрета изменения амплитуды. Поэтому окончания векторов модулированного колебания образуют прямоугольную сетку на фазовой плоскости действительной — Re {Z} и мнимой составляющей вектора модулированного сигнала — Im {Z}. Число узлов этой сетки определяется типом используемого алгоритма QAM. Схему расположения узлов на фазовой плоскости модулированного QAM колебания принято называть созвездием.

Моделирование выполнено для способа модуляции QAM-4, согласно которому в созвездии имеется 4 вершины, имеющие код 00,01,10 и 11. Использован пакет Neural Network программного комплекса MATLAB.

Сеть состоит из входного слоя, скрытого слоя с 10-ю нейронами и выходного слоя. Способ обучения нейронной сети – обучение с учителем с использованием алгоритма Левенберга-Марквардта, который является комбинацией метода Ньютона с методом градиентного спуска.

Процесс обучения нейронной сети завершен за 11 итераций. При этом вектор градиента поверхности ошибок составляет 0.006 к концу последней эпохи.

Распределение функции ошибки (разности между целевым и фактическим значением) совпадает с гауссовским.

Наибольшая плотность вероятности приходится на нулевой промежуток.

Обучающая регрессия при различных параметрах. Целевые значения обозначены пунктирными линиями, фактические значения сплошными цветными. Точками обозначены значения обучающей выборки. Как видно, кривые практически совпадают.

При вводе случайных параметров в качестве входных данных сеть выдает отклик на соответствующий способ демодуляции. Результаты совпадают с ожидаемыми в пределах допустимой погрешности.

Таким образом, аппарат нейронных сетей показал свою состоятельность при решении задачи демодуляции сигналов.

СПИСОК ЛИТЕРАТУРЫ

4. Галкин В.А. Цифровая мобильная радиосвязь. Учебное пособие для вузов.- М.: Горячая линия - Телеком, 2007, -432с.
5. Уоссермен Ф. Нейрокомпьютерная техника.- М.: Мир, 1992, 127с.
6. Брунилин А.А., Бирюков М.А., Саенко И.Б. Модель и метод использования онтологий для управления разграничением доступа в едином информационном пространстве // Математические методы в технике и технологиях – ММТТ. 2016. № 6 (88). С. 122-124.

УДК621.391(075.8)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННОЙ КОМПОНЕНТЫ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Паращук Игорь Борисович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: shchuk@rambler.ru

Аннотация. Предпринята попытка анализа перспектив развития процессов обеспечения безопасности информации относительно новой технологической сферы – киберфизических систем, причем речь идет о защите информации в базовом сегменте систем такого класса – телекоммуникационных сетях. Особое внимание уделено особенностям и сферам применения современных киберфизических систем.

Ключевые слова: *киберфизическая система; Интернет вещей; телекоммуникационная сеть; датчик; сенсор; информационная безопасность.*

INFORMATION SECURITY OF THE TELECOMMUNICATION COMPONENT CYBERPHYSICAL SYSTEMS

Parashchuk Igor
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: shchuk@rambler.ru

Abstract. An attempt has been made to analyze the prospects for the development of information security processes with respect to a new technological sphere – cyberphysical systems, and it is a question of protecting information in the basic segment of systems of this class – telecommunications networks. Particular attention is paid to the peculiarities and spheres of application of modern cyberphysical systems.

Keywords: *cyberphysical system; internetofthings; telecommunication network; detector; sensor; information security.*

Телекоммуникационная компонента представляет собой ключевой элемент (наряду с компонентами вычислений и управления) той составной части киберфизических систем, которая по своей природе дискретна и определяется понятием «кибернетическая». Вторая часть, определяемая понятием «физическая», отвечает за природно-антропогенные системы, которые подчинены базовым законам физики и работают, преимущественно, в непрерывном режиме.

Это сеть телекоммуникаций, основанная на стандартных Интернет-протоколах и предназначенная для взаимодействия датчиков, оборудования и информационных систем в рамках единой информационно-технологической среды, обеспечивающей интеграцию вычислительных ресурсов в физические процессы. Именно эту информационно-технологическую среду, эту информационно-технологическую концепцию в современной научной литературе принято называть киберфизическими системами (CyberPhysical Systems, CPS).

Эти системы должны обладать неразрывной связью между входящими в них вычислительными и физическими элементами. Эту связь обеспечивает телекоммуникационная составляющая киберфизических систем (КФС). Телекоммуникационная компонента уже сейчас активно функционирует, обеспечивая взаимодействие сенсоров, датчиков, оборудования и информационных подсистем КФС в самых разнообразных областях – в космосе, автомобильной, химической промышленности на основе новых технологий, гражданской инфраструктуре, энергетике, здравоохранении, производстве, транспорте, и в некоторых потребительских устройствах. Этот класс систем примято рассматривать как встроенные системы. В них предпочтение отдается вычислительным элементам, и меньше внимания уделяется неразрывной взаимосвязи между

вычислительными и физическими компонентами системы, что, тем не менее, не умаляет значимости телекоммуникационной подсистемы КФС. Вместе с тем, необходимо помнить, что, отличие от традиционных встраиваемых систем, КФС изначально разрабатываются как сеть сравнительно автономных взаимодействующих элементов с физическими входами и выходами, а не как отдельное автономное устройство [1, 2].

Иногда аналитики и эксперты говорят о КФС, как о робототехнических системах, технологиях Интернет-вещей (Internet of Things, IoT) или сенсорных сетях. Необходимо понимать, что это не так, КФС, робототехника, IoT и сенсорные сети – близкие понятия, но не подменяют друг друга. КФС нацелены на углубление связи, взаимопроникновения между вычислительными и физическими элементами технических систем, это позволит увеличить адаптивность, автономность, эффективность, функциональность, надежность, безопасность, и удобство использования таких систем. Именно за эту взаимосвязь и отвечает телекоммуникационная компонента киберфизических систем, которые развиваются в направлении транспортной сферы (предотвращение столкновений), медицины (повышение точности на основе автоматизированной хирургии и медицинского вмешательства наноуровня), чрезвычайных ситуаций (работа в опасных или недоступных средах, поиск и спасение, тушение пожаров, глубоководные исследования), сферы управления и координации действий (диспетчеризация, военная техника), сферы энергетики (энергопассивные здания и сооружения) и иных сферах, нацеленных на расширение способностей человека [3].

Считается, что в киберфизических системах вычислительные элементы через телекоммуникационную компоненту взаимодействуют с датчиками и сенсорами, обеспечивающими мониторинг неких киберфизических показателей, а также с исполнительными элементами, которые вносят изменения в киберфизическую среду. По сути, КФС объединяют информацию от интеллектуальных датчиков, распределенных в физической среде, для лучшего понимания этой среды и выполнения более точных действий.

С точки зрения физики, исполнительные элементы, на основе получаемых данных, вносят изменения в среду обитания пользователей, например, в компьютерном Интернет-пространстве можно использовать КФС для сбора данных о виртуальных действиях пользователей, таких как использование социальных сетей, блогов и сайтов электронной коммерции. В итоге, КФС определенным образом реагируют на такие данные, например, прогнозируя действия или потребности пользователей.

Помимо традиционных подходов, которые имеют место и должны быть использованы для обеспечения информационной безопасности телекоммуникационной компоненты КФС, особое внимание должно быть уделено новому направлению информационной безопасности КФС, связанные с расширением сфер взаимодействия в рамках систем такого класса.

Действительно, некоторые предприятия и организации, взаимоувязанные в единую КФС, зачастую используют системы управления и производства, основанные либо на проприетарных (своих частных, уникальных, защищенных патентом) технологиях или на технологиях связи, не имеющих выход в сеть Интернет.

Однако, по мере расширения связей в рамках КФС, причем связей, использующих открытые стандарты и протоколы телекоммуникаций, рост рисков информационной безопасности неизбежен, для защиты потребуется не только качественная и безопасная связь, но и системы управления учетными записями и системы контроля доступа [4].

Здесь на помощь должен прийти проект, запущенный крупными компаниями в сфере технологий и производства систем защиты информации и ориентированный на проблемы безопасности для КФС (CPS) и (IoT). Проект носит название Cyber Physical Systems Security (CPSSEC) и призван решить проблемы защиты информации в КФС, поскольку и киберфизические системы и IoT играют все более важную роль в критической инфраструктуре, работе правительства и повседневной жизни людей, поскольку эти системы являются источником конкурентного преимущества в современной инновационной экономике и предоставляют широкие возможности для предприятий и организаций безопасности. Вместе с тем, КФС и IoT несомненно увеличивают риски кибербезопасности в целом и риски атак в частности. Последствия непреднамеренных сбоев или злонамеренных атак могут оказать серьезное воздействие на жизнь людей и окружающую среду. Именно поэтому активные и скоординированные усилия необходимы для укрепления безопасности и доверия к киберфизическим системам в целом, и к их ключевой компоненте – телекоммуникационным сетям, в частности.

Заключение. Очевидно, что информационная безопасность КФС не ограничивается безопасностью телекоммуникационной компоненты, политика безопасности должна быть комплексной, всеохватывающей. Вместе с тем она должна учитывать все аспекты информационной безопасности телекоммуникаций в рамках КФС для всех областей приложения этих систем, таких основных сегментов как умное производство, умные сети и услуги, умные здания и инфраструктуры, умный транспорт и умное здравоохранение [4].

Информация, циркулирующая в КФС, в этих умных системах, включающих сети взаимодействующих между собой, через систему телекоммуникаций, вычислительных и физических компонентов, например, таких как датчики, сенсоры, роботы, интеллектуальные здания, медицинские импланты, самоуправляемые автомобили, беспилотные самолеты и др., безусловно должна быть надежно защищена, поскольку от этого зависит безопасность страны.

СПИСОК ЛИТЕРАТУРЫ

1. ФрадковА.Л.Кибернетическаяфизика. СПб: Наука, 2003. – 208 с.
2. Lee E. Cyber Physical Systems: Design Challenges. // University of California, Berkeley Technical Report No. UCB/EECS-2008-08, January 23, 2008.
3. Cyber-physical systems. Program Announcements & Information. // The National Science Foundation, 4201 Wilson Boulevard, Arlington, Virginia22230, USA. 2008-09-30.
4. Черняк Л.В. Киберфизические системы на старте. // Открытые системы. СУБД. – 2014. – № 2. – С. 10-11. URL: http://www.osp.ru/os/2013/10/13039062 (дата обращения: 12.04.2017).

УДК 623.618

ПРОБЛЕМАТИКА ПЛАНИРОВАНИЯ ПРИМЕНЕНИЯ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Пименов Алексей Сергеевич, Деньжонков Кирилл Александрович
Борисов Александр Иванович, Прудников Евгений Константинович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: pima-alex@yandex.ru

Аннотация. В докладе рассматривается проблема отсутствия единого подхода к планированию применения центров обработки данных специального назначения.

Ключевые слова: *методика; хранилище данных; вычислительные узлы; центр обработки данных; специальное назначение.*

PROBLEMS OF PLANNING THE APPLICATION OF DEPO SPECIAL PROCESSING CENTERS

Pimenov Aleksey, Denzhonkov Kirill,Borisov Alexander, Prudnikov Evgeny
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretskiy pr., 3
e-mail: pima-alex@yandex.ru

Abstract. The report discusses the problem of the lack of a unified approach to planning the use of data centers for special purposes.

Keywords: *computing nodes; data processing center; special purpose.*

В настоящее время в мире сложилась нестабильная климатическая и политическая обстановка, которая обязывает находиться в состоянии повышенной готовности к решению задач все органы государственной власти, местного самоуправления и силовые структуры.

В связи с этим как нельзя остро стоит задача доведения информации всем субъектам управления в кратчайшие сроки.

Так 20 сентября 2016 года в городе Ижевск, президент Российской Федерации Владимир Владимирович Путин провел заседание военно-промышленной комиссии. Где отметил необходимость перехода на качественно иной уровень управления, и создания единого информационного пространства, с целью наиболее полного и точного расчета развития складывающейся ситуации и информационной поддержки принятия решения системой управления органов государственной власти, местного самоуправления, силовыми и специальными структурами.

Для выполнения поручений президента РФ и построения эффективной системы управления в настоящее время необходимо использовать ИТ-инфраструктуру.

Одним из элементов базового построения ИТ-инфраструктуры является центр обработки данных (ЦОД) – комплексное организационно-техническое решение, предназначенное для создания высокопроизводительной и отказоустойчивой информационной инфраструктуры.

Как правило, в настоящее время ЦОД состоят из следующих компонентов:

– информационная инфраструктура (серверное оборудование) - выполняет функции хранения и обработки информации;

– телекоммуникационная инфраструктура - выполняет функции связи ЦОД между собой, а также осуществляет передачу данных между ЦОД и глобальной сетью Internet.

– инженерной инфраструктуры.

В свою очередь Информационная инфраструктура состоит из следующих компонентов:

– хранилище данных;

– вычислительные узлы.

Телекоммуникационная инфраструктура (сеть обмена) представляет собой совокупность физических каналов и коммутирующего оборудования.

К инженерной инфраструктуре относится помещение ЦОД, где происходит непосредственно размещение серверного оборудования, как правило, в виде серверных стоек.

Для обеспечения бесперебойной работы центра обработки данных используется система бесперебойного электроснабжения, система кондиционирования воздуха, поддержка постоянной температуры в пределах от 19° до 24°С и влажности от 40 до 80%.

Для минимизации ущерба при техногенных катастрофах, например, при пожаре используется система раннего обнаружения пожара и газового пожаротушения.

Важнейшим параметром функционирования ЦОД является безопасность. В ЦОД так же используются системы видеонаблюдения и физического разграничения доступа.

В настоящее время центры обработки данных получают широкое применение. Они используются как общественные информационные ресурсы и информационные ресурсы органов государственной власти, местного самоуправления, различных силовых и специальных структур.

По характеристике применения ЦОД разделяются на два типа. В основном деление происходит на ЦОД общего использования и ЦОД специального назначения (ЦОД СН). Важнейшими преимуществами создания ЦОД являются консолидация вычислительных мощностей и систем хранения данных.

Наиболее важными в системе функционирования и развития государства являются центры обработки данных специального назначения.

Особенностями ЦОД СН являются:

– обработка информации с различной степенью конфиденциальности;
– воздействие различных внешних факторов, в том числе и деструктивных воздействий;
– наличие специально направленных воздействий;
– необходимость функционирования в особый период;
– обеспечение работы различных категорий пользователей и другие.

Но в настоящее время они подвержены множеству угроз. Эти угрозы могут появляться в результате природных явлений, техногенных аварий и специально направленных воздействий.

В таких условиях качественное планирование применения ЦОД специального назначения является ключевым звеном для эффективного достижения цели.

В сложившейся обстановке, нет единого подхода в планировании применения ЦОД специального назначения, что в итоге является причиной отсутствия типового комплекта документов, направленных на планирование применения ЦОД СН. И в свою очередь, так же, влечет за собой отсутствие системного подхода в управлении инфраструктурой объектов, различные по структуре документы на ЦОД СН, повышенные временные затраты при разработке документов применения и другие недостатки.

Актуальным становится разработка инструментария, позволяющего лицу, ответственному за функционирование ЦОД СН, разработать планирующие документы по его применению и обеспечить их эффективное функционирование.

Появление опыта в виде методики планирования применения ЦОД специального назначения позволит унифицировать управление, предусмотреть восстановление после сбоев и отказов в условиях воздействия на них вероятных угроз.

Решить эту задачу можно, на наш взгляд, путем создания единой методики планирования применения ЦОД специального назначения, которая позволила бы максимально эффективно использовать ЦОД СН, учитывая динамику изменения условий и требований к ним, а также неопределенность исходных данных для принятия решения по применению ЦОД специального назначения.

СПИСОК ЛИТЕРАТУРЫ

1. Спрос на устройства хранения в мире взаимосвязанных данных. // Seagate and BlackArmor, 2015. // [Электронный ресурс]: http://www.seagate.com/ru/ru/tech-insights/demand-for-storage.html.
2. Новые информационные и сетевые технологии в системах управления военного назначения. Часть1. Новые сетевые технологии в системах управления военного назначения. Учебник / Под редакцией С.М. Одоевского. СПб.: ВАС, 2010 – 432 с.
3. Новые информационные и сетевые технологии в системах управления военного назначения.
2. Часть 2. Новые сетевые технологии в системах управления военного назначения. Учебник / Под редакцией И.Б. Саенко. СПб.: ВАС, 2010 – 520 с.

УДК 004.6

ПРИНЦИПЫ МОДЕЛИРОВАНИЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ, ВКЛЮЧАЮЩИХ РАДИОСЕТИ С ПАКЕТНОЙ ПЕРЕДАЧЕЙ ДАННЫХ

Попов Андрей Иванович, Михайличенко Николай Валерьевич
Военная академия связи имени маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: AdPopovAI@yandex.ru, 23esn2008@rambler.ru

Аннотация. В работе рассмотрена радиосеть передачи данных с коммутацией пакетов. Описаны особенности моделирования структуры и варианта способа передачи сообщений в радиосети. Предложен вариант способа уменьшения времени реагирования системы на изменение ее структуры или параметров, а также вариант способа рационального использования имеющихся ресурсов.

Ключевые слова: *радиосеть; сеть передачи данных; коммутация пакетов; моделирование.*

THEMODELING METHODS OF COMMUNICATION NETWORKS WITH PACKET RADIO NETWORKS

Popov Andrey, Mikhaylichenko Nikolay
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: AdPopovAI@yandex.ru, 23esn2008@rambler.ru

Abstract. The paper considers radio communication network with packet switching. The specific facilities of radio network and message communication way modelling described. The way to minimize system reaction time when system structure and parameters changes proposed. The implementation of effective resource using concluded.

Keywords: *radio network; communication network; packet switching; modelling.*

Как известно, сеть передачи данных (СПД) - это система, состоящая из оконечных устройств (терминалов), связанных каналами передачи данных и коммутирующими устройствами (узлами сети), и предназначенными для обмена информационными сообщениями между оконечными пунктами [1]. В свою очередь, по среде распространения СПД разделяется на проводные и радиосети. В радиосетях (или же СПД использующих «радио вставки»), в основе которых лежит радиоизлучение, вопросу оперативного управления структурой радиосети, с учетом её текущего состояния, на наш взгляд уделялось недостаточно внимания.

В рамках предложенного подхода решаются такие вопросы как:

– построение и выбор оптимальной радиотрассы (маршрута);
– гибкая балансировка трафика между маршрутизаторами;
– динамическая оценка плохих и слабы связей;
– оперативное принятие решения на изменение структуры, состояния и текущих тактико-технических характеристик всех элементов, входящих в состав данной системы;
– непрерывный мониторинг состояния узлов-ретрансляторов и каналов связи;
– выбор необходимого и достаточного режима работы источника;
– надежность соединения, за счет: самоорганизующейся, самовосстанавливающейся и самобалансирующейся сети; поддержанием мягкой переадресации; запрещением плохих соединений для оптимизации

При использовании данного подхода необходимо учитывать следующие параметры:

– расстояние до узла-ретранслятора (узла-получателя);
– рельеф местности;
– климатические условия;
– коэффициент затухания;
– диапазон рабочих частот и особенности распространения радиоволн;
– вид и род работы источника радиоизлучения;
– пропускная способность каналов и узлов СПД;
– способ передачи информации;

Так, например, в радиосети для пакетной передачи сообщений нескольким адресатам B_i, в сети с j узлами – ретрансляторами, которые так же могут одновременно являться и узлами-получателями, необходимо использовать направленные антенны. Сложность такого подхода заключается в ограниченном ресурсе мощности радиопередающего устройства и большой площадью антенных полей [2]. Конечно же можно загромоздить помещения аппаратурой и тем самым обеспечить необходимую мощность излучения в том или ином направлении, но при этом ресурс каждого радиопередающего устройства не будет использован в полном объеме, все это при этом будет

сопровождаться значительными финансовыми вложениями как на приобретение оборудования, так и на его текущее обслуживание во время эксплуатации.

Данный подход дает нам:

– возможность создать интегрированную систему, позволяющую практически мгновенно получать данные для оперативного реагирования, управления и анализа;

– возможность получить ряд дополнительных уникальных функций, позволяющих сокращать потери, увеличивать производительность, повышать уровень безопасности технологических процессов;

– средние финансовые организационные затраты при необходимости расширения системы.

В основу предложенного подхода взят принцип достаточности или отсутствия избыточности, что влечет за собой, как правило, повышение эффективности функционирования всей системы в целом. В описанном подходе необходимо иметь сведения о состоянии всех составляющих СПД, что достигается постоянным ее мониторингом [3]. Учитывать так называемые исходные данные (под исходными данными в данном случае понимается состояние СПД в определенный момент времени непосредственно перед передачей того или иного сообщения) [4]. Необходимо сформировать оптимальный маршрут или трассу от узла-источника до узла-получателя. Выбрать необходимый режима работы и мощности излучения.

Таким образом при данном подходе к организации работы СПД с использованием «радио вставок» и выборе необходимой и достаточной мощности излучения можно значительно уменьшать взаимное влияние радиопередающих устройств друг на друга.

СПИСОК ЛИТЕРАТУРЫ

1. Чуднов А.М., Кирик Д.И., Курашев З.В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений/ Радиотехнические и телекоммуникационные системы. - 2017. -№2. с.41-49.
2. Башкирцев А.С., Михайличенко Н.В., Ренсков А.А., Паращук И.Б. Совершенствование объема и номенклатуры множества контролируемых параметров, принадлежащих пространству управления информационными системами и сетями // Успехи современной науки 2017, №1, Т.4, С.46-52.
3. Бирюков М.А. Разработка модели нарушителя правил разграничения доступа к единому информационному пространству // Математические методы в технике и технологиях – ММТТ. 2017. Т. 3. С. 107-110
4. Саенко И.Б., Бирюков М.А. Методика интеграции локальных схем разграничения доступа к разнородным ресурсам единого информационного пространства // Информационные технологии в управлении (ИТУ-2016) Материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В.Г. Пешехонов. 2016. С. 758-762.

УДК 004.45:004.067.04

МЕТОД РАНДОМИЗИРОВАННЫХ СВОДНЫХ ПОКАЗАТЕЛЕЙ ДЛЯ ЭКСПЕРТНОЙ ОЦЕНКИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Попова Елена Владимировна
Смольный институт Российской академии образования
Россия, Санкт-Петербург, Полюстровский пр., 59
e-mail: serana5@inbox.ru

Аннотация. В статье анализируются методы многокритериальной оптимизации для подбора наилучшего варианта системы защиты информации. Делается вывод о методе рандомизированных сводных показателей, как наиболее подходящем, нуждающемся в дальнейшей модификации.

Ключевые слова: *многокритериальная оптимизация; сводный показатель; система защиты информации.*

METHOD OF RANDOMIZED CONSOLIDATED INDICATORS FOR EXPERT EVALUATION OF INFORMATION PROTECTION SYSTEMS

Popova Elena
Smol'nyj Institut RAO
Rossija, Sankt-Peterburg, Poljustrovskij pr., 59
e-mail: serana5@inbox.ru

Abstract. The article analyzes the methods of multicriteria optimization for the selection of the best variant of the information security system. The conclusion is made about the method of randomized aggregates as the most appropriate in need of further modification.

Keywords: *multi-criteria optimization; summary indicator; information security system.*

Методы многокритериальной оптимизации более полно отражают задачи, ставящиеся перед реальными многосвязными системами, которыми являются системы защиты информации (СЗИ). Перед лицом, принимающим решение, появляется проблема выбора наиболее подходящего метода многокритериальной оптимизации, и, как следствие, принятие допущений, условностей, границ теоретических аналогов реальных объектов. Ставится задача выбора оптимального варианта СЗИ,

который спроектирован для конкретного предприятия. Оптимизация проводится по нескольким критериям: равнозначным, независимым, наиболее полно отражающим объекты выбора.

Рассмотрим различные способы выбора оптимизационного варианта. На основе проведённого анализа выберем метод, соответствующий поставленной задаче и имеющий минимальные недостатки. При построении траектории выбора наилучшего варианта есть соблазн сократить количество вариантов, например, до множества Парето, убрав заведомо худшие. Согласно принципу Эджворта-Парето [1], при многокритериальном выборе один вариант лучше другого, если по одному частному критерию он лучше другого, а по остальным не хуже. Сформированное множество Парето не больше первоначального количества вариантов, и задача нахождения наилучшего варианта, как кажется, упрощается. Но наилучшие решения могут лежать за пределами множества Парето, если не выполняются определённые условия использования принципа, например, аксиома транзитивности, в которой говорится, что отношение предпочтения должно быть транзитивным бинарным отношением.

Ещё один путь упрощения задачи – сокращение количества критериев. Метод главного критерия уменьшает множество критериев до одного [2]. Один критерий объявляется главным, по нему ищется экстремум, а остальные критерии формируют ограничения. Один из главных недостатков метода – это допустимая область решения может оказаться пустым множеством.

Метод уступок [2] преодолевает недостаток предыдущего метода. Критерии оцениваются по значимости и используются в порядке возрастания. Выбирается первый критерий и решается однокритериальная задача. Затем находят величину возможного отклонения. Не выходя за размеры фиксированных отклонений, итерационно находятся следующие экстремальные задачи. В конце используют последний критерий, и решается задача, аналогичная задаче с главным критерием. При достижении граничных условий решение может быть слабо эффективным.

Метод свёртки применяют при агрегировании всех критериев в скалярную величину, и на основании этой величины происходит оценивание объекта [3]. Свёртка имеет аддитивный или мультипликативный вид. Мультипликативная запись зависит от уменьшения значений отдельных критериев и может стремиться к нулю. При аддитивной свёртке уменьшение значений некоторых критериев компенсируется увеличением других, имеющих большую «весомость». Мультипликативную свёртку можно перевести в аддитивную, логарифмируя произведение.

Немаловажным этапом метода свёртки является задача выбора весовых коэффициентов, которая допускает различные решения. Метод логического анализа основан на прямом экспертном присвоении конкретных значений критериям. Эксперты присваивают значения критериям в диапазоне натурального ряда от единицы до величины количества критериев [4]. Весовые коэффициенты считаются как отношение суммы присвоенных значений разными экспертами одному критерию к общей сумме по всем критериям и по всем экспертам. В случае разной компетентности экспертов, им присваиваются экспертные коэффициенты, которые включаются в формулы. В этом методе важны не только правильно подсчитанные экспертные коэффициенты, но и достаточное количество экспертов.

Метод анализа иерархий [4] основан на построении матриц парных сравнений различных критериев. Матрица должна быть квадратная, обратно-симметричная и согласованная. Оценивается критерий натуральными числами от 1 до 9. Диагональные элементы после нормализации и образуют весовые коэффициенты. При построении первоначальной матрицы, если критерий менее важен его значение оценивается обратным числом. Таким образом, важный критерий с оценкой n и менее важный с оценкой $\frac{1}{n}$, симметрично расположенные относительно диагонали, отличаются в n^2 раз, где $n\epsilon\{1,\dots,9\}$, что является грубым приближением.

Формулы Фишберна [4] дают аналитическую запись весовых коэффициентов. Если критерии упорядочены в порядке убывания, то предлагается применить арифметическую или геометрическую убывающую прогрессию. Весовые коэффициенты, полученные с помощью простых формул, кажутся очень привлекательными, но, во-первых, не во всех задачах критерии подчинены отношению порядка, и, во-вторых, встаёт вопрос обоснования применения формул прогрессий.

К методу свёртки относится метод сводных показателей (МСП). Существует вектор исходных характеристик исследуемого объекта $\boldsymbol{x} = (x_1, \dots, x_m)$. $q_i(x_i)$– отдельные показатели объекта. $\boldsymbol{w} = (w_1, \dots, w_m)$ - вектор весовых коэффициентов. $Q(q_1, \dots, q_m; \boldsymbol{w})$- сводный показатель исследуемого объекта. В методе рандомизированных сводных показателей (МРСП) неопределённость задания весовых коэффициентов компенсируется их рандомизацией [5,6]. Весовые коэффициенты имеют совместное равномерное распределение на области допустимых значений. Рандомизированный сводный показатель представляет собой случайную величину, у которой можно подсчитать математическое ожидание $\bar{Q}^{(j)} = M\tilde{Q}^{(j)}$, стандартное отклонение $S^{(j)} = \sqrt{D\tilde{Q}^{(j)}}$ и достоверность доминирования $P\left(\{\tilde{Q}^{(m)} > \tilde{Q}^{(l)}\}\right) > \alpha$.. Для увеличения точности и достоверности оценок применяют дополнительную нечисловую, неполную и неточную информацию, то есть ннн-информацию (I).

Рассмотрим различные модификации МРСП. Из перечисленных методов наиболее подходящим к решению задачи выбора наилучшего варианта СЗИ по равнозначным независимым критериям является метод свёртки с рандомизированными весовыми коэффициентами, то есть МРСП.

МРСП подвергается изменениям при решении специфических задач. Одним из способов модификации МРСП является применение модели с иерархической системой критериев [7], где на каждом уровне решаются локальные задачи, а итоговые результаты объединяются на самом высоком уровне. На нулевом уровне строятся несколько сводных показателей, которые делят критерии на подзадачи.

Сводные показатели следующего уровня формируются на основе показателей предыдущего уровня. Происходит декомпозиция сложной задачи на более простые подзадачи.

Недостатком данной модификации является потенциальная сложность разбивки на подзадачи. Используется принцип сильных и слабых связей. То есть связи между сводными показателями, формирующими показатель более высокого уровня должны быть сильнее, чем с другими показателями «своего» уровня.

Также происходит увеличение дисперсии с переходом на следующий иерархический уровень. При формировании сводных показателей на всех иерархических уровнях для повышения точности оценок формируется экспертами дополнительная ннн-информация. Но эксперту психологически трудно оценить сводные показатели на разных уровнях, имеющие сложные связи.

В другой работе [8] формируются два различных набора оценок объектов в определённые промежутки времени, сформированные двумя экспертными группами. Итоговые результаты (более высокий иерархический уровень) получают как усреднение предыдущих результатов. Для этого метода необходимо двойное количество экспертов с одинаковыми оценками компетентности, и расчёт допустимых границ согласованности действий экспертов как внутри группы, так и между группами.

Во всех работах, с описанием практических расчётов применения МРСП, в основе вычислений использовались точные данные об исследуемых объектах, полученные из печатных источников, котировок, электронных документов [9,10]. Количественные оценки разных свойств одного объекта затем подвергались нормировке и подстановке в формулы метода.

При исследовании СЗИ, спроектированной для конкретного предприятия точные данные, характеризующие её показатели по критериям, например, конфиденциальности, целостности, доступности информации невозможно найти в каких-либо источниках.

Поэтому необходима новая модификация МРСП, подходящая для выбора наилучшего варианта СЗИ с учётом возможности использования точного результата в критериальных формулах.

Заключение.

МРСП выбран как наиболее подходящий для решения поставленной задачи нахождения наилучшего варианта СЗИ.

Подбирая подходящую модификацию данного метода, можно добиться количественного обоснования полученных результатов по критериям, коррелирующим с показателями бизнес-процессов предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Ногин В. Д. Обобщённый принцип Зджворта-Парето и границы его применимости // Экономика и математические методы, «Издательство Наука», М. 2005. С. 128-134.
2. Городецкий С. Ю. ННГУ. Учебный курс «Модели и методы конечномерной оптимизации». Часть 2. Нелинейное программирование и многоэкстремальная оптимизация. // Учебно-исследовательская лаборатория "Математические и программные технологии для современных компьютерных систем (Информационные технологии)". 2003. 157 с.
3. Герасимова Л.В., Погожев И.Б. Комплексная оценка качества проектов и выбор оптимального варианта по методу академика А.Н. Крылова // Стандарты и качество. 1972. №8. С.37-39.
4. Постников В. М. Спиридонов С. Б. Методы выбора весовых коэффициентов локальных критериев // Наука и Образование. МГТУ им. Н. Э. Баумана, Электрон. журн. 2015. № 06. С. 267-287.
5. Хованов Н.В., Федотов Ю.В. Модели учета неопределенности при построении сводных показателей эффективности деятельности сложных производственных систем // Научные доклады НИИ менеджмента СПбГУ. 2006. № 28. 37 с.
6. Hovanov N., Yudaeva M., Hovanov K. “Multicriteria estimation of probabilities on basis of expert non-numeric, non-exact and non-complete knowledge // Abstracts of 18-th International Conference on Multiple Criteria Decision Making”. Chania (Greece), June 19-23, 2006. P.102.
7. Михайлов М. В. Модель оценки качества институтов высшего профессионального образования // Вестник Санкт-Петербургского университета. Сер. 5. Вып. 4. 2006. С. 74-82.
8. Жук С.Н. Оценка эффективности функционирования сложных систем по иерархической системе показателей // Труды СПИИРАН. 2013. Вып. 26. С. 194-203.
9. Корников В. В., Серегин И. А., Хованов Н. В. Многокритериальное оценивание финансовых рисков в условиях неопределённости: Учеб. Пособие. СПб.: Изд-во С.-Петерб. Ун-та, 2002. 96 с.
10. Хованов Н. В., Федотов Ю. В. Модели учёта неопределённости при построении сводных показателей эффективности деятельности сложных производственных систем // Научные доклады № 28(R)-2006. СПб.: НИИ Менеджмента СПбГУ, 2006. 31 с.

УДК 623:681.3

ВЫБОР МЕТОДА ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ ДЛЯ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ

Прудников Евгений Константинович, Пименов Алексей Сергеевич, Ащеулов Сергей Викторович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: piramida-17@mail.ru

Аннотация. Сформулирована необходимость выбора параметров корректирующего кода и алгоритмов его использования для обеспечения требуемых значений показателей достоверности в системах передачи данных.

Ключевые слова: *помехоустойчивое кодирование; достоверность передачи.*

ELECTRONICS OF THE INTERFERENCE CODIFICATION FOR DATA TRANSMISSION CHANNELS

Prudnikov Evgeny, Pimenov Aleksey, Asheulov Sergey
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretskiy pr., 3
e-mail: piramida-17@mail.ru

Abstract. The article states the need to select the parameters of the algorithms used to ensure the required values of reliability indication in data transmission systems.

Keywords: *noise-immune input; authenticity of the transfer.*

Проблема обеспечения достоверности и своевременности передачи информации в сетях имеет большое значение.

Если при передачи обычной телеграммы в тексте возникает ошибка или при разговоре по телефону слышны помехи, то в большинстве случаев ошибки и искажения легко исправляются по смыслу. При передаче данных одна ошибка на тысячу переданных сигналов может серьезно отразиться на качестве информации. Временные же показатели при передачи данных учитываются лишь по среднему времени передачи, либо не учитываются вообще.

Причин возникновения ошибок при передаче данных две:

– техническое состояние каналов связи и коммутационного оборудования сети;

– помехи, возникающие в каналах связи различной физической природы, а также внешние воздействия при передаче информации.

Выделяются три основных метода борьбы с ошибками:

– использование свойств корректирующего (помехоустойчивых) кодов;

– использование систем повышения достоверности;

– комбинированный метод.

При рассмотрении эффективности помехоустойчивого кодирования в качестве основных показателей используются скорость и достоверность передачи.

Однако эти показатели рассматриваются либо с учетом среднего времени передачи, либо без учета временных показателей, характеризующих задержки сообщений при передаче их от отправителя к получателю. Кроме того, не принимаются во внимание вероятности ложного выделения сигнала из шумов канала связи либо трансформации одной разрешенной кодовой комбинации в другую разрешенную.

Обеспечение помехоустойчивости передачи сообщений может производиться как с помощью безизбыточных, так и корректирующих кодов.

Использование безизбыточного кода предполагает многократное повторение комбинации и применение на приемной стороне мажоритарной обработки принятой последовательности безизбыточных кодовых комбинаций определенной длины с установленной кратностью повторения, что обеспечивает исправления ошибок.

Корректирующий код может использоваться в режимах обнаружения, исправления, а также обнаружения и частичного исправления ошибок.

В режиме обнаружения ошибок вероятность ошибочного приема меньше, чем в режиме исправления ошибок. Кроме того, обнаружение ошибок по своей природе является более простой задачей и не требует сложной реализации.

Однако в случае обнаружения ошибок в принимаемой последовательности комбинаций требуется стирание принятой последовательности и ее повторной передаче путем запроса по обратному каналу и накопления нового безошибочного отрезка последовательности требуемой длины, что может привести к большим временным задержкам при передаче сообщения.

Таким образом, для систем передачи данных требуется выбирать параметры корректирующего кода и алгоритм его использования для обеспечения требуемых значений показателей достоверности, а с другой стороны необходимо учитывать временные параметры доведения

информации до получателя, что особенно важно при передаче сигналов, имеющих важность и срочность доведения.

СПИСОК ЛИТЕРАТУРЫ

1. Дадаян Ю.Д. Помехоустойчивое кодирование. Учебное пособие для студентов (2009 г., с. 22, 34-45).
2. Фрейман В.И. Теория электрической связи. Помехоустойчивое кодирование в телекоммутационных системах (изд. ПНИПУ, 2011 г., с 43-58).

УДК 004.056

АНАЛИЗ ПРОБЛЕМЫ КОНТРОЛЯ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ

Саенко Игорь Борисович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mail: ibsaen@mail.ru

Аннотация. В работе рассматривается проблема контроля доступа к информационным ресурсам в облачных инфраструктурах. Анализируются возможности перспективных моделей контроля доступа к информации, известных в научной литературе, и оценивается их возможность и эффективность применения в облачных вычислительных системах. Формулируются направления решения поставленной проблемы и пути их реализации.

Ключевые слова: *модель контроля доступа; облачная инфраструктура; ролевое управление доступом; генетический алгоритм.*

ASSESSMENT ANALYSIS OF THE PROBLEM OF INFORMATION RESOURCES ACCESS CONTROL IN CLOUDY INFRASTRUCTURES

Saenko Igor
St. Petersburg Institute for Informatics and Automation of RussianAcademy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
e-mail: ibsaen@mail.ru

Abstract. The paperconsiders a problem of information resources access control in cloudy infrastructures. Possibilities of the perspective models of information access control known in scientific literature are analyzed, and their possibility and efficiency of application in cloudy computing systems is evaluated. The directions of solving of the delivered problem and the ways of their implementation are formulated.

Keywords: *access control model, cloudy infrastructure, role-based access control, genetic algorithm.*

Облачные инфраструктуры представляют собой сравнительно новый вид компьютерных инфраструктур, которые притягивают к себе повышенное внимание. Однако более широкому распространению этой технологии препятствуют проблемы безопасности. Настоящая работа посвящена анализу проблемы контроля доступа к информационным ресурсам в облачных инфраструктурах.

Недостатком большинства существующих облачных инфраструктур является отсутствие возможности гибкого управления со стороны пользователей доступом к своим данным, что вызвано универсальностью решений по контролю доступа, принимаемых поставщиками облачных услуг [1]. Неоднородность и большое разнообразие ресурсной среды облачного хранилища требуют всестороннего и детально проработанного механизма контроля доступа, чтобы обеспечить динамические, постоянно расширяемые и хорошо настраиваемые требования по защите информации пользователей [3].

Однако существующие механизмы безопасности, обеспечиваемые поставщиками облачной инфраструктуры, не удовлетворяют этим требованиям [3]. Кроме того, проблема безопасности информации в облачных инфраструктурах обостряется, если используются открытые веб-сервисы [5]. Все это настоятельно требует проработки вопросов совершенствования политик контроля доступа и моделей, лежащих в их основе [6, 7].

Анализируя модели контроля доступа к информации, которые применяются в облачных инфраструктурах, можно сделать вывод, что наибольшей популярностью обладает модель RBAC, в дополнение к которой предлагается использовать некоторые более перспективные модели.

В [6], кроме RBAC, анализируются и предлагаются к использованию модель ABAC и модель «множественной аренды» (multi-tenancy), являющаяся разновидностью OrBAC.

В [4] предлагается использовать основанную на RBAC модель Amazon Web Services (AWS), позволяющую расширить возможности политик RBAC и облегчить интеграцию службы разграничения

доступа в корпоративные приложения. В [3] предлагается гибкая междоменная модель контроля доступа, основанная на механизмах преобразования ролей.

В [7] среди анализируемых моделей доступа присутствуют MAC и DAC, но сразу же отмечается их низкая эффективность в облачных инфраструктурах.

В качестве наиболее приемлемых предлагается использование моделей RBAC и ABAC. В [5] предлагается модель, основанная на политиках (Policy-based Access Control), которая является разновидностью модели OBAC.

В [2, 4] предлагается реализовать новую парадигму услуг, связанную с разграничением доступа, «контроль доступа как сервис» (access control as a service) с использованием применяемых в облачных инфраструктурах моделей доступа.

Вопросы оценки, формирования и оптимизации политик разграничения доступа в научной литературе в наибольшей степени проработаны для модели RBAC, так как она допускает строгую формализацию с выделением переменных, целевой функции и ограничений. Это позволило выделить задачу оптимизации политики разграничения доступа на основе RBAC в отдельный класс задач интеллектуального анализа данных (Data Mining), получившего название Role Mining Problem (RMP) [8]. Разработаны различные варианты постановки этой задачи и предложен ряд методов и алгоритмов их решения [9].

В качестве более общего подхода для решения задач RMP предлагается использовать генетические алгоритмы. Генетические алгоритмы, как и другие алгоритмы биоинспирированной оптимизации, следует рассматривать как достаточно эффективные средства решения задач оптимизации политик разграничения доступа.

Таким образом, анализ поставленной проблемы позволяет сделать следующие выводы:

1) проблема разграничения доступа в облачных инфраструктурах вызвана спецификой свойственных им угроз безопасности и является достаточно актуальной;

2) данная проблема обостряется в критически важных информационных системах;

3) решения этой проблемы связывается с использованием наряду с традиционной моделью контроля доступа RBAC новых перспективных моделей ABAC, OrBAC, OBAC и других, построенных на их основе;

4) разработка новых моделей, методов и алгоритмов для решения задач оценки, оптимизации, верификации и реконфигурации политик безопасности, основанных на моделях контроля доступа, является активно развивающимся научным направлением, в котором использование интеллектуальных методов, в частности генетических алгоритмов, эвристических многоагентных систем и т.д. позволит получить достаточно эффективные решения.

Для получения решений, направленных на устранение рассмотренной проблемы, необходимо проведение детального анализа существующих работ и нормативных документов в предметной области безопасности облачных инфраструктур, а также применение методов системного анализа, математического моделирования и искусственного интеллекта, теории защиты информации, программной инженерии, объектно-ориентированного проектирования и анализа и других теорий.

Работа выполнена при финансовой поддержке РФФИ (проект 15-07-07451) и при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007.

СПИСОК ЛИТЕРАТУРЫ

1. Саенко И.Б., Бирюков М.А., Ефимов В.В., Ясинский С.А. Модель администрирования схем разграничения доступа в облачных инфраструктурах // Информация и космос, 2017. – №1. – С. 121-126.
2. Fotiou, N., Machas, A., Polyzos, G.C. etal. Access control as a service for the Cloud // J. Internet Serv. Appl. 2015, Vol.6, No.11. doi:10.1186/s13174-015-0026-4
3. Ullah S., Xuefeng Zh., Feng Zh. TCloud: A Dynamic Framework and Policies for Access Control across Multiple Domains in Cloud Computing // International Journal of Computer Applications (0975 – 8887), Vol. 62, No.2, January 2013, pp.1-7.
4. WuR., Zhang X., Ahn G.-J. et al. ACaaS: Access Control as a Service for IaaS Cloud // URL: http://sefcom.asu.edu/publications/design-implementation-access-science2013.pdf (датаобращения: 13.09.2017).
5. Patel S.Ch., Umrao L.S., Singh R.Sh. Policy-based Access Control in Cloud Computing // Proceedings of the International conference on Artificial Intelligent and Soft Computing, December 2012.
6. Meghanathan N. Review of Access Control Models for Cloud Computing // Proceedings of the Third International Conference on Computer Science, Engineering & Applications, ICCSEA, Chennai, India, pp. 77-85, May 24-26, 2013. DOI: 10.5121/csit. 2013.3508.
7. Majumder A., Namasudra S., Nath S. Taxonomy and Classification of Access Control Models for Cloud Environments / Z. Mahmood (ed.) // Continued Rise of the Cloud, Computer Communications and Networks, DOI 10.1007/978-1-4471-6452-4_2, 2014, pp.23-32.
8. Frank M., Buhmann J.M., Basin D. On the Definition of Role Mining // Proceedings of the 15th ACM symposium on access control models and technologies (Pittsburgh, PA, USA, June 09 - 11, 2010). SACMAT '10. ACM, New York, NY, 2010, pp.35-44.
9. Vaidya J., Atluri V., Guo Q. The Role Mining Problem: Finding a Minimal Descriptive Set of Roles // Proceedings of the 12th ACM symposium on Access control models and technologies (Sophia Antipolis, France, June 20 - 22, 2007). SACMAT '10. ACM, New York, NY, 2007, pp.175-184.

УДК621.391(075.8)

РАЗРАБОТКА МЕТОДА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ВЫБОРУ АППАРАТНО-ПРОГРАММНЫХ МОДУЛЕЙ ДОВЕРЕННОЙ ЗАГРУЗКИ В ИНТЕРЕСАХ ЗАЩИТЫ ОТ НСД НА АРМ ДОЛЖНОСТНЫХ ЛИЦ СИЛОВЫХ ВЕДОМСТВ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Саяркин Леонид Андреевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: sayarkin95@mail.ru

Аннотация. Рассмотрены типы современных средств доверенной загрузки и особенности подходов к формулировке понятия «доверенная загрузка». Проанализирована роль различных средств доверенной загрузки в структуре системы защиты и функции, реализуемые ими для разных уровней архитектуры компьютера в составе автоматизированного рабочего места администратора или пользователя телекоммуникационной сети.

Ключевые слова: *доверенная загрузка; автоматизированное рабочее место; уровень; защита; доступ; функции.*

DEVELOPMENT OF A METHOD TO SUPPORT DECISION-MAKING ON THE CHOICE OF HARDWARE AND SOFTWARE MODULES TRUSTED BOOT TO PROTECT AGAINST UNAUTHORIZED ACCESS TO WORKSTATION OF OFFICIALS OF LAW ENFORCEMENT AGENCIES IN TELECOMMUNICATION NETWORKS

Sayarkin Leonid
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: sayarkin95@mail.ru

Abstract. Types of modern means of trusted loading and features of approaches to the formulation of the concept of "trusted download" are considered. The role of various means of trusted loading in the structure of the protection system and the functions implemented by them for different levels of the computer architecture in the automated workplace of the administrator or the user of the telecommunications network is analyzed.

Keywords: *trusted download; the automated workplace; level; protection; access; functions.*

В конце 20 века, перейдя на новую ступень развития в области инфотелекоммуникационных технологий, человечество осознало, что для внедрения их в повседневную жизнь необходима стойкая система защиты своего автоматизированного рабочего места (АРМ), ибо утрата информации может дорого обойтись как развитию страны, так и уровню ее безопасности [1].

Процесс модернизации технического оборудования затронул не только национальные и государственные организации нашей страны. Изменения коснулись и Вооруженных сил Российской Федерации.

Обладая конфиденциальной информацией или информацией, содержащей сведения государственной тайны, необходимо обеспечить надежную защиту АРМ от несанкционированного доступа (НСД) в области информационной безопасности (ИБ).

Информационная безопасность – есть основа всей системы безопасности автоматизированных систем ВС РФ. Именно она позволяет обеспечивать конфиденциальность, целостность и доступность информации. ИБ характеризуется отсутствием недопустимого риска, связанного с утечкой информации вследствие НСД. Об ИБ в ВС РФ и ее важности впервые было отмечено в Доктрине информационной безопасности Российской Федерации, утвержденной Президентом РФ 9 сентября 2000 года [2, 3].

С внедрением в Вооруженные силы компьютерной техники появилась необходимость не только защита от кражи сведений, составляющих государственную тайну, противником, но и защита вычислительной техники (ВТ) от возможных сетевых атак, с последующим выводом ее из строя.

Поэтому помимо организации информационной защиты вычислительной техники от НСД в целом, как минимум, необходимо организовать все меры для надежного и безопасного запуска ее отдельных компонентов [4].

Относительно не так давно был предложен совершенно новый способ реализации данного процесса.

Аппаратно-программные модули доверенной загрузки (АПМДЗ) – основное решение данной проблемы.

На сегодняшний день их большое разнообразие позволяет подобрать АПМДЗ практически для любых целей, что является огромным достоинством к применению на разных видах АРМ в ВС РФ. Но не стоит забывать о том, что не каждый модуль доверенной загрузки может быть использован в Вооруженных силах, т.к. в основном аппаратная часть импортного производства.

Соответственно, для того, чтобы модули могли успешно функционировать в системе ВС РФ, необходимо пройти освидетельствование в органах ФСБ и ФСТЭК.

Некоторые АПМДЗ позволяют блокировать НСД к компьютеру еще на уровне BIOS, что не позволяет запуск ОС с внешнего носителя. Это является очень большим достоинством [5].

Необходимость ВС РФ в АПМДЗ, очевидна, т.к., на мой взгляд, ни одно другое средство не способно защитить компьютер как на аппаратном, так и на программном уровнях одновременно.

Таким образом, существующие типы средств доверенной загрузки предназначены для определенных целей и уровней защищаемых элементов АРМ, а их применение должно осуществляться комплексно, с учетом уровня существующих угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Требования к средствам доверенной загрузки. // Информационное письмо ФСТЭК России от 06.02.2014 №240/24/405 «Об утверждении Требований к сдедствам доверенной загрузки» в соответствии с Приказом ФСТЭК России от 27.09.2013 №119). [Электронный ресурс]:http://fstec.ru/normotvorcheskaya/793.
2. Никитин Е.А., Шрамко В.А. Всегда ли на замке? Как обезопасить компьютер модулем доверенной загрузки. // Vikotenik. №20 (Август), 2010. // [Электронный ресурс]: http://vikotenik.livejournal.com/226909.html.
3. Конявский В.А. Управление защитой информации на базе СЗИ НСД «Аккорд». – М.: Радио и связь, 1999. – 325 с.
4. Саенко И.Б., Бирюков М.А., Ефимов В.В., Ясинский С.А. Модель администрирования схем разграничения доступа в облачных инфраструктурах // Информация и космос. – 2017. – №1. – С. 121-126.
5. Левенков О.А. Средства доверенной загрузки. // Технологии безопасности. №6, 2013 С. 40-41.

УДК 623.618

ОБЪЕДИНЕННАЯ АРХИТЕКТУРА БЕЗОПАСНОСТИ ДЛЯ ЗАЩИТЫ КОРПОРАТИВНОЙ СЕТИ

Селяков Максим Николаевич, Пащенко Василий Владимирович,
Беденков Виктор Николаевич, Матвеев Александр Николаевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: maxolga801@mail.ru

Аннотация. В сегодняшнем мире подключенное к сетям предприятие сталкивается с парадоксом с точки зрения безопасности. Именно открытость и повсеместность, благодаря которым Интернет стал мощным средством ведения бизнеса, налагают на его пользователей и огромные обязательства. Интернет был создан для совместного пользования, а не для защиты. Порты и порталы, приглашающие удаленные узлы, мобильных пользователей, клиентов и партнеров по бизнесу в надежную внутреннюю сеть, также потенциально приглашают и кибер-воров, хакеров и прочих лиц, готовых к злоупотреблениям сетевыми ресурсами с целью получения личной выгоды. Единственной эффективной стратегией сетевой безопасности является такая стратегия, которая бы пронизывала архитектуру от края к краю и обеспечивала выполнение корпоративных принципов на многих уровнях и во многих точках в сети. Поэтому создание безопасных сетей, данных - комплексная стратегия, направленная на решение актуальных задач, стоящих перед специалистами в области безопасности информационных технологий.

Ключевые слова: *корпоративная сеть;архитектуры безопасности; конфиденциальность информации.*

UNITED ARCHITECTURE OF SECURITY FOR PROTECTION OF THE CORPORATE NETWORK

Selyakov Maxim,Pashchenko Vasily,Bedenkov Victor,Matveyev Alexander
Military Academy of Communications. Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: maxolga801@mail.ru

Abstract. In today's world, an enterprise connected to networks faces a paradox in terms of security. Openness and ubiquity, thanks to which the Internet has become a powerful means of doing business, impose huge obligations on its users. The Internet was created for sharing, not for protection. Ports and portals that invite remote sites, mobile users, customers and business partners to a reliable internal network also potentially invite cyber thieves, hackers and others who are ready to abuse network resources for personal gain. The only effective network security strategy is a strategy that permeates architecture from edge to edge and ensures the implementation of corporate principles at many levels and at many points in the network. Therefore, the creation of secure networks, data - a comprehensive strategy to address the pressing challenges faced by experts in the field of information technology security.

Keywords: *corporate network; security architecture; confidentiality of information.*

Цель данного исследования - разработка и совершенствование объединенной архитектуры безопасности для защиты корпоративной сети.

Комплексная стратегия безопасности основана на следующих основных принципах:

1. Многоуровневая безопасность, определяющая функции защиты на прикладном уровне,

уровне безопасности с сетевой поддержкой и уровне сетевой безопасности.

2. Безопасность с изменяемой глубиной охвата в масштабе предприятия и не только на границе с Интернетом.

3. Управление политикой замкнутого цикла, включая постоянное развитие политики для соответствия меняющимся требованиям бизнеса, условиям в сети и отраслевой базе знаний.

4. Унифицированное управление доступом путем строгой аутентификации и авторизации на детализированном уровне, которые управляются и определяются централизованно в масштабе всего предприятия.

5. Безопасные сетевые операции за счет физического или логического разделения сетевого управления и пользовательского трафика.

6. Безопасные мультимедийные коммуникации, защищенные высокопроизводительным шифрованием и туннелированием.

7. Выживание в случае атаки, например, за счет применения упругих архитектур, в которых отсутствует единая точка выхода из строя, и применения систем обнаружения атак, антивирусного программного обеспечения, фильтрации содержания и постоянной бдительности по мере принятия атакующими новых средств на вооружение.

Нарушения защиты и неправомерный доступ к конфиденциальным данным могут стоить предприятиям огромных затрат, но требование сетевой безопасности не ограничивается лишь финансовыми стимулами. Правительства многих стран заставляют предприятия выполнять определенные нормы в отношении сетевой безопасности и защиты.

Взломщики пользуются широким арсеналом средств и способов нанесения ущерба сети. С помощью этих средств они могут инициировать многоуровневые атаки для получения доступа к сети, создав сначала точку доступа для вторжения в сеть, а затем - вторичные атаки для использования прочих частей сети.

Организации должны относиться к безопасности как к устойчивому процессу и развивающемуся способу мышления о том, как защитить системы, сети, приложения и ресурсы, как понизить риск путем постоянного и стабильного прогресса в поиске и устранении уязвимых мест и пробелов в политике безопасности. Корпорации и государственные учреждения должны уметь определять масштабы угрозы при сбоях в работе мер безопасности, уметь обнаруживать нарушения защиты и справляться с ними.

Объединенная архитектура безопасности определяет виртуальные частные сети, виртуальные локальные вычислительные сети, брандмауэры, шифрование и прочие механизмы, которые позволяют предприятиям снизить риски, связанные с Интернет-соединением, модернизирует программы и инфраструктуры корпоративной безопасности в соответствии с требованиями бизнеса, этики и нормативных актов и с целью обеспечения целостности данных и конфиденциальности, обнаруживает различные средства взломщиков, определяет виды атак и средства их предотвращения и борьбы с ними, рассматривает угрозы на многих функциональных и архитектурных уровнях, позволяя предприятиям гибко определять, что необходимо защитить, от какого рода угроз, как это осуществить и на каких уровнях.

Учитывая законодательные акты о конфиденциальности данных, постоянно меняющуюся среду сетевых угроз и уязвимых мест, а также тот факт, что коллективы, специализирующиеся на обеспечении безопасности в информационных технологиях работают в условиях ограниченных бюджетов и людских ресурсов, многие предприятия передают некоторые или все функции безопасности под ответственность сертифицированных специалистов в области безопасности.

Услуги по консалтингу в области безопасности помогут предприятию уверенно двигаться с целью:

– достижения и обеспечения соответствия Акту Грэмма-Лича-Блайли;

– акту о праве перевода и сохранения медицинского страхования и ответственности и прочим законодательным актам;

– получения объективной валидации разработок, политики и практики в области безопасности от третьих сторон;

– получения общей информации о безопасности в результате тщательного анализа уязвимых мест в сети, общего обзора объектов, где расположены беспроводные узлы, добавляемые к проводной сети, а также представления прочих услуг в области безопасности.

Организации, работающие в секторе здравоохранения, финансовом и страховом секторе, были бы заинтересованы в получении любых или всех нижеперечисленных услуг, связанных с недавно принятыми федеральными законодательными актами:

– оценка и анализ существующей сети и среды с целью обеспечения соответствия новым отраслевым нормам;

– разработка планов работ в тех областях, в которых соответствие не обеспечивается;

– реализация политики, процедур, процессов и технологий, обеспечивающих соответствие новым стандартам;

– сертификация соответствия организационной структуры предприятия нормам и законодательным актам;

– контроль с целью обеспечения постоянного соответствия.

Выводы.Принципы, на которых основана объединенная архитектура безопасности, предоставляют предприятиям план реализации решений безопасности, обеспечивающих целостность и конфиденциальность информации применительно ко всему ряду сетевых приложений и архитектур, включая защиту от внешних атак, злоупотреблений приложениями, вирусов, несанкционированного доступа, перехвата или манипуляций данными в пути следования.

Благодаря принятым решениям предприятия могут защищать ответственные бизнес-ресурсы и с уверенностью и конфиденциальностью пользоваться Интернетом как дополнением к своей надежной внутренней сети.

СПИСОК ЛИТЕРАТУРЫ

1. В. Олифер «Компьютерные сети: принципы, технологии, протоколы», Учебник для ВУЗОВ.
2. Э. Таненбаум «компьютерные сети» 4-е издание Москва - 2003.
3. Альянах И.Н. «Моделирование вычислительных систем»: Учебное пособие – Л.: Машиностроение. Ленингр. Отделение, 1988 - 223с.
4. Локальные вычислительные сети: Справочник, Кн.1. Принципы построения, архитектура, коммуникационные средства»: под редакцией С.В. Назарова– М.: Финансы и статистика, 1994 - 208с.

УДК621.391(075.8)

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В ПРИЛОЖЕНИЯХ НА ПЛАТФОРМЕ ASP.NET

Скрябин Евгений Андреевич, Зайцев Данила Евгеньевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: skryabin.ev@yandex.ru

Аннотация. В работе рассматриваются основные способы защиты данных в автоматизированной системе контроля и учета успеваемости обучающихся Высших учебныхзаведений**.** Согласно используемой платформе и средствам разработки, в качестве одного из таких способов предлагается использовать метод цепочного хеш-связывания для защиты от модификации исходного кода программы. Метод основан на внедрении хеш-функций в программный код и использовании определенных машинных инструкций.

Ключевые слова: *автоматизированная система; платформа; машинная инструкция; веб-сервер; хеш-функция.*

METHODSOFINFORMATIONPROTECTION IN APPLICATIONS ON THE ASP.NET PLATFORM

Skryabin Evgeny, Zajcev Danila
S.M.Budjonny Military Academy of the Signal Corps
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: skryabin.ev@yandex.ru

Abstract. The article deals with the main methods of data protection in the automated system for monitoring and recording the academic performance of students of the Higher Educational Institutions. One of these processes is used the method of chain hash-binding to protect against modification of the source code of the program according to the used platform and development tools. The method is based on the implementation of hash functions in the program code and the use of certain machine instructions.

Keywords: *automated system; platform; machine instruction; web-server; hash-function.*

В качестве приложения на платформе ASP.NET предлагается рассмотреть автоматизированную систему, разработанную на языке программирования C# с использованием системы управления базой данных (СУБД) Microsoft SQL Server и используемую в Высших учебных заведениях для контроля и учета успеваемости обучающихся. ASP.NET - это технология создания web-приложений и web-сервисов от компании Microsoft. Она является составной частью платформы Microsoft .NET и развитием более старой технологии Microsoft ASP. C# - объектно-ориентированный язык программирования. Использование подобной автоматизированной системы в ВУЗах обусловлено необходимостью интеграции больших массивов разносторонних данных и информационных потоков между подразделениями вузов. Кроме того, это способствует организации информационной поддержки и сопровождению образовательного процесса, проведению оценки учебной работы и деятельности сотрудников, а также оптимизации рабочего и учебного процессов и снижению трудоёмкости, сокращения «бумажного» документооборота, повышению обоснованности оценок. Данное приложение представляет собой электронный журнал, с помощью которого администратор может редактировать расписания занятий по группам и факультетам, а

преподаватель через личный кабинет выставляет оценки студентам по различным дисциплинам. Также функционал данной системы позволяет формировать необходимые отчеты, отображающие данные в виде таблиц или диаграмм.

Следует отметить такой важный момент, что, поскольку приложение на платформе ASP.NET выполняется на центральном процессоре, а исполняемый код в - оперативном запоминающем устройстве (ОЗУ) в открытом виде, это также создает угрозу для безопасности приложения. На основе этого предлагается использовать защиту, заключающуюся в применении хеш-функций для контроля целостности. Предполагается, что данная система защиты должна обладать такими свойствами, как: защитой программы от модификации до и после загрузки в ОЗУ; распределенностью кода, реализующего защиту; неотделимостью кода; сокрытием логики работы программы; алгоритмической сложностью; затруднением исследования программы; прозрачностью защиты [1].

Разработанный метод основан на применении цепочного хеш-связывания. Так как в работе рассматривается платформа ASP.NET, то для этого предлагается ввести следующие обозначения, используя команды промежуточного языка CIL [2]:

– Instruction (data) – общий вид машинной инструкции, где в качестве аргумента выступают данные - data. Результатом выполнения такой инструкции является изменение содержимого регистра флагов или регистров процессора;

– Block – блок линейно выполняющихся машинных инструкций;

– IL_XXX: – метка кода, символьное представления адреса;

– br addr (IL_XXX) – безусловный переход в программе по указанному адресу addr или метке IL_XXX;

– Aggregate (заполнитель) – данные, к которым не происходит обращение в рамках рассматриваемого перехода;

– HF (хеш-функция) – реализация алгоритма вычисления некоторой хеш-функции в машинных командах. Аргументами функции являются данные программы.

Порядок, в котором располагаются блоки инструкций, не критичен. Содержимое заполнителя и его объем могут быть любыми.

Для выполнения цепочного хеш-связывания исходная хеш-функция должна по заданному аргументу, которым является исполняемый код, рассчитать адрес, на который нужно перейти программе. Исходный вид хеш-функции можно представить в виде стандартного полинома. При выполнении программы с самого начала, как правило, уже известны пары аргументов и значений функции. Следовательно, имеется возможность рассчитать значения параметров хеш-функции.

Метод цепочного хеш-связывания основан на разделении исполняемого кода на определенные блоки инструкций разного размера. К окончанию каждого блока добавляется связка хеш-функция – безусловный переход, а между блоками вставляется заполнитель. Перед заполнителем обязательно расположена команда безусловного перехода. Соответственно, после выполнения данной команды процессор выполняет следующий блок инструкций, а целостность программы и ее функционал не нарушаются [3].

В качестве аргументов хеш-функции выступает исполняемый код, либо участки программы, содержащие данные. Помимо инструкций текущего блока, аргументами могут быть и инструкции любого другого блока. После выполнения хеш-функция определяет адрес, по которому осуществляется переход к другому участку программы. Главным моментом является то, что, если хешируемый код не был изменен, то адрес осуществляемого перехода будет корректным. В противном случае – программа обратится по неверному адресу, и операционная система завершит работу программы [4]. Для полной защиты от модификации кода необходимо условие активности хотя бы одной из всех используемых функций. В этом случае предложенный метод полностью работает.

Однако, при использовании данного подхода можно также столкнуться с одной из проблем. Большое количество внедренных хеш-функций замедляет работу программы, несмотря на улучшенную защищенность. Поэтому необходимо правильно регулировать соотношение защищенности и скорости исполнения.

В результате были рассмотрены основные способы защиты как самого приложения, реализованного на платформе ASP.NET, так и его данных. Основным достоинством при использовании метода цепочного хеш-связывания является затруднение анализа программного кода и необходимость снятия защиты при помощи отключения всех хеш-функций.

СПИСОК ЛИТЕРАТУРЫ

1. Безопасность веб-приложений ASP.NET [Электронный ресурс]. Общие сведения об угрозах безопасности – Режим доступа: https://msdn.microsoft.com/ru-ru/library, свободный. – Загл. с экрана. – Яз. Рус.
2. Троелсен, Э. Язык программирования C# 5.0 и платформа .NET 4.5[Текст] / Э.Троелсен. – Москва: Вильямс, 2015. – 1312 с.
3. Кукарцев, А.М., Лубкин, И.А. Методика защиты программного кода от несанкционированной модификации и исследования посредством его хеширования[Текст] / А.М. Кукарцев, И.А Лубкин. – Красноярск: СибГАУ, 2008. – 56 – 60 с.
4. Баранов В.В., Бирюков М.А., Кравченко С.А., Максимов А.С., Саенко И.Б. Имитационная модель для анализа рисков информационной безопасности при проектировании ролевых схем разграничения доступа к базам данных // Актуальные проблемы обеспечения информационной безопасности. Труды межвузовской научно-практической конференции. 2017. С. 26-31.

УДК 004.732

О ПРОБЛЕМЕУПРАВЛЕНИЯ ВИРТУАЛЬНЫМИ ЛОКАЛЬНЫМИ ВЫЧИСЛИТЕЛЬНЫМИ СЕТЯМИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Старков Артем Михайлович, Саенко Игорь Борисович
Военная академия связи имени Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: kadet58v@mail.ru, ibsaen@mail.ru

Аннотация. Обоснована проблема управления виртуальными локальными вычислительными сетями в корпоративных информационных системах. Предложена постановка задачи на разработку модели и методики формирования и реконфигурации структуры VLAN, а также пути ее решения.

Ключевые слова: *корпоративная информационная система; локальная вычислительная сеть;VLAN.*

ABOUT THE PROBLEM OF CONTROL OF THE VIRTUAL LOCAL COMPUTER NETWORKS IN CORPORATE INFORMATION SYSTEMS

Starkov Artyom, Saenko Igor
Military telecommunication academy
Russia, St. Petersburg, Tikhoretskiy pr., 3
e-mails: kadet58v@mail.ru, ibsaen@mail.ru

Abstract. The problem of control of the virtual local computer networks in corporate information systems is justified. Task statement for development of model and technique of formation and reconfiguration of VLAN structure and also a way of its solving are offered.

Keywords: *corporate information system; local area network; VLAN.*

Построение и функционирование корпоративных информационных систем (КИС) имеют целью повышение эффективности взаимодействия сотрудников в организации и эффективности реализации информационных процессов. Основу построения КИС составляют локальные вычислительные сети (ЛВС) организации. От решений, принятых по построению и функционированию ЛВС, существенно зависит эффективность функционирования КИС и организации в целом. Одним из перспективных способов повышения эффективности построения и функционирования ЛВС является применение технологии «виртуальной локальной вычислительной сети» (virtual local area network – VLAN). Технология VLAN обычно рассматривается как средство повышения информационной безопасности в КИС. Однако при разумном проектировании и управлении структурой VLAN эта технология позволяет также получить выигрыш по пропускной способности и другим характеристикам качества. Поэтому целью настоящей работы является обоснование проблемы управления VLAN в КИС, постановка задачи на разработку научно-методического обеспечения процессов проектирования и/или реконфигурирования структуры VLAN и определение путей ее решения.

Согласно ГОСТ Р 52653-2006 и ГОСТ РВ 51987-2002 корпоративная информационная система представляет собой разновидность автоматизированной системы управления, доступ к которой имеет ограниченный круг лиц, определенный ее владельцем или соглашением участников этой системы.

Основой построения КИС являются компьютеры, объединенные с помощью ЛВС. От эффективности функционирования ЛВС зависит как эффективность КИС, так и эффективность работы организации или предприятия в целом. На эффективность функционирования ЛВС оказывают влияние множество факторов. При этом одними из основных факторов являются выбор подхода к построению ЛВС и управление ею. Выбранная архитектура построения ЛВС и модель управления ею должны удовлетворять особенностям КИС и выполнять требования, предъявляемые к ней.

Для решения данной задачи существует несколько подходов. При этом одним из наиболее перспективных подходов является применение технологии VLAN [1].

Данная технология позволяет более эффективно использовать возможности ЛВС, что заключается в увеличении пропускной способности сети, обеспечении удобства реконфигурации сети, независимости логической структуры ЛВС от физического размещения станций, повышении уровня защиты информации, возможности управления логической структурой ЛВС и удобстве администрирования сети. В результате повышается своевременность предоставления услуг абонентам КИС.

В настоящее время при проектировании схем построения VLAN применяются эмпирические рекомендации [2], где виртуальные подсети образуются вокруг серверов различного назначения и охватывают компьютеры, имеющие право работать с этими серверами, а также с учетом организационной структуры предприятия. Однако в условиях высокой динамики развития КИС разработка схемы построения VLAN, основанная на эмпирических рекомендациях, становится достаточно затруднительна. В процессе трансформации VLAN возможен дисбаланс показателей

функционирования сети, что существенно осложняет выбор наилучшего варианта организации ЛВС, т.к. показатели функционирования ЛВС должны отвечать предъявляемым требованиям [3].

В соответствии с руководящими документами к управлению ЛВС предъявляются требования по устойчивости, непрерывности и оперативности, а также реализация в КИС следующих уровней управления: организационного, оперативно-технического и технологического [4].

Технологию VLAN следует относить к технологическому уровню управления в виду того, что к числу основных задач этого контура управления связью относятся выбор маршрутов передачи сообщений, коммутация каналов связи и соединение абонентов между собой, изменение режимов работы средств связи, контроль состояния и диагностика технических средств и другие.

Таким образом, постановку задачи на разработку научно-методического обеспечения процессов проектирования и/или реконфигурирования структуры VLAN, включающего в себя модель и методику управления VLAN в КИС, может быть сформулирована следующим образом.

В качестве исходных данных учитываются следующие факторы:

1) структура ЛВС, характеристики входящих в ее состав технических и программных средств;
2) требования по устойчивости, надежности и оперативности управления сетью;
3) перечень оцениваемых показателей эффективности функционирования сети;
4) перечень задач, решаемых с помощью ЛВС КИС;
5) структура информационно-технического взаимодействия должностных лиц в КИС;
6) категории срочности передачи информации в сети.

Задача имеет следующие ограничения и допущения:

1) коммутационное оборудование (коммутаторы, маршрутизаторы) поддерживает применение технологии VLAN;
2) матрица доступа между абонентами задается политикой безопасности корпорации;
3) рассматривается взаимодействие в рамках ЛВС КИС, взаимодействие с другими КИС не рассматривается;
4) не рассматриваются климатические факторы и деструктивные воздействия;
5) не рассматривается возможность влияния специальных программных воздействий.

Требуется разработать следующие компоненты научно-методического обеспечения:

1) модель функционирования ЛВС на технологии VLAN, которая адекватно реагирует на решения по построению VLAN и ее реконфигурацию;
2) методику формирования и реконфигурации структуры VLAN, позволяющую перейти от предыдущей к новой конфигурации VLANс минимальными временными затратами и с обеспечением требуемых функциональных показателей по пропускной способности и своевременности предоставления услуг абонентам КИС.

Для разработки модели функционирования ЛВС на технологии VLAN предполагается использовать развитые инструментальные средства имитационного моделирования.

Сравнительный анализ известных средств такого вида показал, что наиболее подходящим средством имитационного моделирования для разработки модели выступает программная система AnyLogic [5].

Для разработки методики формирования и реконфигурации структуры VLAN представляется целесообразным использовать алгоритмы генетической оптимизации, позволяющие формировать структуру VLAN с учетом множества предъявляемых к ней функциональных требований [6].

Предложенная постановка задачи на разработку научно-методического обеспечения процессов проектирования и/или реконфигурирования структуры VLAN направлена на разработку соответствующих модели и методики, реализация которых позволит повысить эффективность функционирования всей КИС в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Демин И.В. Методы анализа корпоративной вычислительной сети, построенной по технологии VLAN. Диссертация на соискание ученой степени кандидата технических наук. – М.: Московский государственный институт электроники и математики (технический университет), 2002. – 119 с.
2. Ермаков А.Е. Основы конфигурирования корпоративных сетей Cisco.– М.: ФГБОУ «УМЦ ЖДТ», 2013. – 247 с.
3. Авраменко В.С., Козленко А.В.Модель для количественной оценки защищенности информации от несанкционированного доступа в автоматизированных системах по комплексному показателю // Труды СПИИРАН. – 2010. – № 2 (13). – С. 172-181.
4. Арсланов Х.А. Автоматизированная система управления связью в Вооруженных Силах Российской Федерации и приоритетные направления ее развития. [Электронный ресурс] / Х.А. Арсланов, А.С. Башкирцев, А.М. Лихачев. – Режим доступа: http://www.army.informost.ru/2016/pdf/1-5.pdf (дата обращения 01.08.2017).
5. Саенко И.Б., Бирюков М.А., Ефимов В.В., Ясинский С.А. Модель администрирования схем разграничения доступа в облачных инфраструктурах // Информация и космос. – 2017. – №1. – С. 121-126.
6. Саенко И.Б., Котенко И.В. Применение средств генетической оптимизации и визуального анализа для формирования схем доступа в ВЛВС // Информационные технологии и вычислительные системы. – 2015. – №1. – С. 33-46.

УДК 641.2

АНАЛИЗ НАЗНАЧЕНИЯ ОСНОВНЫХ ФУНКЦИЙ, РЕАЛИЗУЕМЫХ В ПРОЦЕССЕ УПРАВЛЕНИЯ УС СН

Сутырин Вячеслав Геннадьевич, Хмелевской Валерий Павлович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: svg346@mail.ru, h02v08p@rambler.ru

Аннотация. В докладе рассмотрены основные функции, реализованные в процессе управления узлом связи.

Ключевые слова: *узел связи специального назначения, функции управления, организация управления, система управления.*

ASSIGNMENT ANALYSIS OF KEY TASKS IN THE MANAGEMENT OF THE COMMUNICATION NODE A SPECIAL PURPOSE

Sutyrin Vyacheslav, Khmelevskoy Valerij
Millitary Academy of Communications named S.M. Budyonnogo
Russia, St. Peterburg, Tikhoretsky pr., 3
e-mails: svg346@mail.ru, h02v08p@rambler.ru

Abstract. The paper describes the main functions implemented in the management of the communication node.

Keywords: *node special purpose, management functions, management organization, management system.*

Главной задачей узла связи специального назначения (УС СН) является обеспечение своевременного прохождения заданного потока сообщений по управлению войсками (силами) как в повседневной деятельности, так и в боевой обстановке с требуемой достоверностью и безопасностью.

Для успешной реализации целей и задач функционирования УС СН, определенных в боевом приказе, на узле связи организуется управление. Сущность организации управления заключается в разработке, подготовке и реализации комплекса мероприятий по созданию системы управления, реализующей процесс управления УС СН. Система управления УС СН представляет собой совокупность органов управления (ОУ) УС СН, пунктов управления (ПУ) узлом связи и его элементами и средств технической основы управления УС СН (средства связи и автоматизации). Должностные лица (ДЛ) ОУ УС СН осуществляют преобразование информации о состоянии УС СН и внешней среды в командную информацию управления. Сбор информации о состоянии управляемых объектов и внешней среды, ее преобразование в командную информацию и доведение команд и распоряжений до подчиненных ДЛ ОУ УС СН осуществляют с использованием средств управления. Таким образом, управление узлом связи заключается в целенаправленной деятельности ДЛ ОУ по поддержанию высокой боевой и мобилизационной готовности узла связи, всесторонней его подготовке к обеспечению связи и руководству узлом связи при выполнении поставленных задач.

Целью управления УС СН является обеспечение наиболее эффективного использования сил и средств узла связи при выполнении поставленных перед ним задач.

Цели функционирования УС СН достигаются путем выполнения определенных функций управления, которые, в свою очередь, реализуются последовательным решением совокупности задач управления.

Под функцией управления понимается существенно влияющая на реализацию предназначения и целостности системы деятельность лица, принимающего решение по формированию и использованию информационного ресурса, характеризующего состояние или группу состояний объекта управления.

К основным функциям управления УС СН целесообразно отнести:

– учет;
– контроль;
– планирование;

Регулирование (оперативное управление).

При этом, успешная реализация функции «Учет» определяет степень реализации остальных функций управления УС СН, таких, как «Контроль», «Планирование» и «Регулирование». Управленческие задачи, решаемые при выполнении функции «Учет», обеспечивают получение полной и достоверной информации о состоянии объектов управления и внешней среды, без которой невозможно выполнение остальных функций управления для обеспечения требуемых значений. Поэтому функция «Учет» является одной из важнейших функций управления, так как именно она в

значительной степени определяет значения таких показателей процесса управления УС СН, как устойчивость, непрерывность, оперативность и скрытность.

Функция «Учет» обеспечивает представление ДЛ ОУ УС СН в удобном для восприятия виде информацию, характеризующую текущее состояние УС СН в целом, отдельных его элементов и внешней среды, первичную обработку введенных данных, их накопление и выдачу.

Содержанием функции управления «Контроль» является сравнение истинного и требуемого состояния контролируемого объекта (УС СН и его элементов) и принятие решения о необходимости выработки управляющих воздействий на него. Результаты выполнения функции «Контроль» инициализируют выполнение функции «Планирование» в процессе организации боевого применения УС СН на организационном уровне управления связью, либо инициализируют выполнение функции «Регулирование (Оперативное управление)» на оперативно-техническом уровне управления связью.

«Планирование», как функция управления, направлено на разработку такой системы мероприятий по организации боевого применения узла связи в целом и отдельных его элементов, выполнение которых обеспечило бы реализацию цели функционирования УС СН. При этом определяется порядок и сроки проведения указанных мероприятий. Кроме того, осуществляется выбор и обоснование критериев оценки состояния УС СН, по которым можно было бы судить о степени достижения целей функционирования УС СН.

Реализация функции управления «Регулирование (оперативное управление)» заключается в оценке несоответствия текущего состояния УС СН запланированному, разработки вариантов устранения несоответствия с учетом имеющихся ресурсов связи и принятия решение на приведение состояния УС в соответствие с запланированным на основе одного из разработанных вариантов.

Таким образом, управление УС СН представляет собой систему целенаправленных, взаимоувязанных между собой действий должностных лиц органов с использованием средств управления, на которых они решают задачи управления, по обеспечению эффективной эксплуатации узла связи (элементов узла связи) в мирное время, при приведении в высшие степени боевой готовности и в военное время в соответствии с заданными целями функционирования.

СПИСОК ЛИТЕРАТУРЫ

1. Анфилатов В.С. Теоретические основы автоматизации управления войсками и связью. Часть 1. Системные основы автоматизации управления войсками и связью: Учеб. пособие. – СПб.: ВАС, 2014. – 312с.
2. Анфилатов В.С., Авраменко В.С., Пантюхин О.И. Теоретические основы автоматизации управления войсками и связью. Часть 2. Основы построения и функционирования систем автоматизации управления войсками и связью: Учеб. пособие. – СПб.: ВАС, 2015г. – 304с.
3. Новые информационные и сетевые технологии в системах управления военного назначения. Часть 1. Новые информационные технологии в системах военного назначения. Учебник. Под редакцией С.М. Одоевского. – СПб.: ВАС, 2010. 432с.
4. Бушуев С.Н., Авраменко В.С., Копчак Я.М., Козленко А.В. Методологические аспекты оценки качества управления связью. – «Вопросы радиоэлектроники», 2013. Т. 3. № 1. С. 49-53.

УДК 641.2

ТРЕБОВАНИЯ К ВОЗМОЖНАСТЯМ ФУНКЦИИ «УЧЕТ», РЕАЛИЗУЕМОЙ ПРИ ОРГАНИЗАЦИИ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ УЗЛОМ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Сутырин Вячеслав Геннадьевич, Хмелевской Валерий Павлович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails:svg346@mail.ru,h02v08p@rambler.ru

Аннотация. Рассмотрена реализация функции «Учет», в различных режимах функционирования, в процессе управления узлом связи специального назначения.

Ключевые слова: *узел связи специального назначения, функции управления, организация управления, система управления.*

REQUIREMENTS VOZMOJNOSTYAM FUNCTION "ACCOUNTING", IMPLEMENTED WITH AUTOMATION MANAGEMENT NODE A SPECIAL PURPOSE

Sutyrin Vyacheslav, Khmelevskoy Valerij
Millitary Academy of Communications named S.M. Budyonnogo
Russia, St. Peterburg, Tikhoretsky pr., 3
e-mails: svg346@mail.ru,h02v08p@rambler.ru

Abstract.Inthe article, consideration of the regime of «Accounting» in various modes of operation in the process of managing a special-purpose communication node.

Keywords: *node special purpose, management functions, management organization, management system.*

Цели функционирования узла связи специального назначения (УС СН) достигаются путем выполнения определенных функций управления (учет, контроль, планирование, регулирование (оперативное управление)), каждая из которых реализуется последовательным решением совокупности задач управления.

Функция «Учет» обеспечивает представление должностным лицам органов управления (ДЛ ОУ) УС СН в удобном для восприятия виде информацию, характеризующую текущее состояние УС СН в целом, отдельных его элементов и внешней среды. Учету подлежит следующая информация:

– данные о планируемом состоянии УС и его элементов;
– данные о текущем состоянии УС и его элементов;
– данные о текущем состоянии внешней среды;
– данные о прогнозируемом состоянии УС и его элементов;
– данные о прогнозируемом состоянии внешней среды;
– данные о наличии резерва сил и средств УС и его элементов;
– команды управления, указания и распоряжения по связи;
– нормативно-справочная информация.

В составе сведений о внешней среде должна присутствовать следующая информация:

– состояние старшей системы (системы связи), в составе которой функционирует УС СН и ее требования к значениям характеристик существенных свойств узла связи;
– возможности противника по воздействию на УС СН в целом и его элементы, процессы их функционирования;
– климатические и физико-географические условия функционирования УС и его элементов [1].

Сбор и учет указанной выше информации может осуществляться в соответствии с одним из реализуемых в конкретный момент времени режимов: по расписанию (регламенту), по запросу системы управления и по событию в управляемом объекте.

При реализации режима «По расписанию (регламенту)», сбор и учет информации состояния осуществляется через определенные, возможно равные (по таймеру), промежутки времени, определяемые руководящими документами по организации связи или при планировании боевого применения УС СН.

При реализации режима «По запросу системы управления», сбор и учет информации состояния инициируется системой управления УС по различным причинам, например, по запросам должностных лиц органов управления УС в процессе выполнения ими функции управления «Контроль» или при резком изменении состояния внешней среды: существенные изменения состояния старшей системы (системы связи), воздействия противника и т.п [2-4].

При реализации режима «По событию в управляемом объекте», сбор и учет информации состояния инициируется управляемым объектом при резком изменении его состояния.

Как отмечалось выше, для успешной реализации функции управления «Учет» информация состояния, подлежащая учету, должна быть предварительно собрана. Для организации сбора информации о текущем состоянии объекта управления и внешней среды, на УС СН (его элементах) создается специальная система сбора информации. Структура этой системы должна соответствовать структуре системы управления УС.

В любом случае основу информации состояния управляемого объекта, составляют объективные данные о текущем состоянии основных средств, участвующих в образовании каждой связи. Таким образом, объектами контроля состояния связи, являются:

– радиолинии;
– линии передачи (линий радиорелейной, тропосферной, спутниковой и проводной связи по наличию необходимого уровня приема контрольного сигнала или синхронизации аппаратуры разделения каналов);
– пары линий передачи;
– каналообразующая аппаратура;
– системы передачи;
– линейные тракты;
– аппаратура разделения/объединения каналов (потоков);
– групповые тракты;
– каналы системы передачи;
– кроссовая аппаратура;
– аппаратура вторичного уплотнения;
– спецаппаратура;
– абонентские линии;
– оконечная аппаратура телефонной, телеграфной, факсимильной связи и передачи данных.

Информация о состоянии перечисленных объектов контроля собирается на уровне технологического управления связью (на боевых постах элементов УС) вручную или автоматически, в зависимости от уровня развития и возможностей применяемых на УС средств технологического

управления передавать свое состояние и воспринимать управляющие воздействия по технологическим каналам управления.

Таким образом, проведенный анализ показал, что функция учет, является наиболее важной и сложной, с точки зрения ее технической реализации, при организации управления узлом связи специального назначения, в различных режимах функционирования.

СПИСОК ЛИТЕРАТУРЫ

1. Анфилатов В.С. Теоретические основы автоматизации управления войсками и связью. Часть 1. Системные основы автоматизации управления войсками и связью: Учеб. пособие. – СПб.: ВАС, 2014.
2. Анфилатов В.С., Авраменко В.С., Пантюхин О.И. Теоретические основы автоматизации управления войсками и связью. Часть 2. Основы построения и функционирования систем автоматизации управления войсками и связью: Учеб. пособие. – СПб.: ВАС, 2015г.
3. Новые информационные и сетевые технологии в системах управления военного назначения. Часть 1. Новые информационные технологии в системах военного назначения. Учебник. Под редакцией С.М. Одоевского. – СПб.: ВАС, 2010.
4. Бушуев С.Н., Авраменко В.С., Копчак Я.М., Козленко А.В. Методологические аспекты оценки качества управления связью. – «Вопросы радиоэлектроники», 2013. Т. 3. № 1.

УДК 004.056

ПОДХОД К ПОСТРОЕНИЮ ИМИТАЦИОННОЙ МОДЕЛИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОБОТОТЕХНИЧЕСКОГО КОМПЛЕКСА

Теплов Иван Андреевич, Махнач Андрей Валерьевич, Саенко Игорь Борисович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: iteplov95@gmail.com, gyfte@yandex.ru, ibsaen@mail.ru

Аннотация. Предлагается подход к построению имитационной модели функционирования системы информационной безопасности робототехнического комплекса. Для решения поставленной задачи предлагается использовать программное средство имитационного моделирования AnyLogic.

Ключевые слова: *имитационная модель; робототехнический комплекс; система информационной безопасности; система массового обслуживания.*

AN APPROACH TO CREATION OF THE SIMULATION MODEL FOR THE ROBOTIC COMPLEX INFORMATION SECURITY SYSTEM

Teplov Ivan, Mahnach Andrey, Saenko Igor
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: iteplov95@gmail.com, gyfte@yandex.ru, ibsaen@mail.ru

Abstract. An approach to creation of a simulation model for the robotic information security system. For solving that task, it is proposed to use the AnyLogic software of simulation modeling.

Keywords: *simulation model; robotic complex; information security system; queuing system.*

В последние годы происходит роботизация практически всех сфер человеческой деятельности. Диапазон применения робототехники является чрезвычайно широким. Так, робототехнические комплексы (далее РТК) вытесняют человека на производстве [1]. Полная автоматизация многих технологических процессов сводит участие людей в производстве к принятию важных решений и устранению возникающих неисправностей оборудования. РТК используются при исследованиях космического пространства и океанских глубин. С помощью роботов проводятся сложнейшие хирургические операции на мозге и сердце. В силу внедрения РТК в военной области военная техника становится все умней и самостоятельней. Управление движением, контроль обстановки, прицеливание и поражение цели производит машина, а человеку остаются решение тактических задач и техническое обслуживание [2].

Важной частью РТК является система информационной безопасности (СИБ) [3]. СИБ предназначена для обеспечения информационного контроля программного обеспечения и технической составляющей РТК, локализации и выявления аномального поведения в информационно-технической составляющей РТК.

Для разработки и планирования применения СИБ РТК целесообразно использовать имитационную модель. Это обусловлено рядом причин. Во-первых, традиционные расчетные математические методы требуют применения высокой степени абстракции и не учитывают важные детали. Имитационная модель позволяет описать структуру системы и ее процессы в естественном виде, не прибегая к использованию формул и строгих математических зависимостей. Во-вторых, имитационная модель обладает возможностями визуализации процесса работы системы во времени, схематичного задания ее структуры и выдачи результатов в графическом виде. Это позволяет наглядно представить полученное решение. Наконец, в-третьих, возможность в реальности оценить

эффективность системы можно лишь через месяцы или даже годы. Имитационная модель позволяет определить оптимальность таких изменений за считанные минуты, необходимые для проведения эксперимента.

Опишем алгоритм работы модели. В качестве источников информации (далее ИИ) для РТК выступает Оператор. Все моменты установления связи между РТК и Оператором могут быть детерминированными или случайными. В детерминированных процессах обмена данными события формируются через определенные промежутки времени. Случайные процессы имеют заранее заданные законы распределения. Поток информации, поступающий от Оператора к РТК и наоборот, рассмотрим в виде трафика, характеризующегося величиной потока и объёмом информации. Трафик записывается в оперативную память (ОП), которая служит очередью и имеет ограниченный объем.

Из очереди заявки поступают на обслуживание в обслуживающее устройство, роль которого играет процессор (ПР). В зависимости от загруженности ПР и объема ОП, заявки будут обрабатываться в соответствии с используемыми службами с некоторой интенсивностью обслуживания.

После обработки трафика ПР распределяет данные трафика в соответствии со службами с некоторой интенсивностью и производит их регистрацию в журнале трафика по службам. При этом учитываются номер сессии и номер данных службы. Аналогичный процесс проходит и на системе Оператора.По окончанию сессии, установленной между Оператором и РТК, СИБ отсылает копию журнала трафика Оператору. Модель учитывает числовые данные по службам, которые являются аналогами объема, поступающего на них трафика. СИБ Оператора, в свою очередь, представляет мощную вычислительную систему, на которой происходит анализ и сравнение журналов Оператора и РТК.

Для разработки имитационной модели СИБ РТК предлагается использовать программное средство AnyLogic, которое поддерживает различные подходы к созданию имитационных моделей: процессно-ориентированный (дискретно-событийный), системно динамический и агентный, а также любую их комбинацию [4, 5].

Уникальность, гибкость и мощность языка моделирования, предоставляемого AnyLogic, позволяет учесть любой аспект моделируемой системы с любым уровнем детализации. Графический интерфейс AnyLogic, инструменты и библиотеки позволяют быстро создавать модели для широко спектра задач от моделирования производства, логистики, бизнес-процессов до стратегических моделей развития компании и рынков.

СПИСОК ЛИТЕРАТУРЫ

1. Шурков В. Н. Основы автоматизации производства и промышленные роботы: Учебное пособие для машиностроительных техникумов // В. Н. Шурков. – М.: Машиностроение, 1989.
2. Авраменко В.С. Адаптивный контроль защищенности информации от несанкционированного доступа на основе информационных образов // Проблемы информационной безопасности. Компьютерные системы. 2010. № 2. С. 45-49.
3. Батанов А.Ф., Грицынин С.Н., Муркин С.В. Робототехнические комплексы для обеспечения специальных операций // Научно-технический журнал «Специальная техника». – URL: http://www.bnti.ru/showart.asp?aid=456&lvl=02.01.02.02 (дата доступа: 10.05.2017).
4. Котенко И.В., Саенко И.Б. SIEM-системы для управления информацией и событиями безопасности // «Защита информации. Инсайд». – №5, 2012. – С.54-65.
5. Инструмент имитационного моделирования AnyLogic: обзор.– URL: http://www.anylogic.ru/overview (дата доступа: 10.05.2017).

УДК 004.056.57

ПОДХОД К ОБОСНОВАНИЮ ТРЕБОВАНИЙ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Тесля Сергей Петрович, Мартынюк Иван Анатольевич, Федорова Светлана Владимировна,
Чоп Алексей Андреевич
Военная академия связи имени МаршалаСоветского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail:ivanmartin88@yandex.ru

Аннотация. В докладе рассматривается обоснование требований к средствам защиты ИТКС от комплекса целенаправленных воздействий – компьютерных атак.

Ключевые слова: *информационно-телекоммуникационная сеть; средства защиты информации; компьютерная атака.*

APPROACH TO THE RATIONALE OF REQUIREMENTS TO THE PROTECTION RESOURCES OF THE INFORMATION AND TELECOMMUNICATION NETWORK

Teslia Sergey, Martynyuk Ivan, Fedorova Svetlana, Chop Aleksey
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Peterburg, Tihoreckyav., 3
e-mail: ivanmartin88@yandex.ru

Abstract. The report describes the rationale for the requirements to the protection resources of information and telecommunications networks from the complex targeted attacks.

Keywords: *information and telecommunications network; protection resources; computer attack; cybernetic attack; networks security.*

Высокие требования, предъявляемые к уровню защищенности информационно-телекоммуникационной сети (ИТКС), предопределяют необходимость проведения оценки эффективности системы защиты информации.

Принято считать, что эффективность системы защиты ИТКС определяется только эффективностью средств защиты, что неверно. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

– средства разграничения доступа к информации в автоматизированных системах (паролирование);

– средства защиты информации при передаче ее по каналам связи (межсетевые экраны, криптомаршрутизаторы);

– средства защиты от информационного воздействия программ-вирусов (антивирусные системы и системы обнаружения вторжений) [1].

Это означает, что ни одно отдельно выбранное средство защиты информации не может защитить ИТКС от комплекса целенаправленных воздействий - компьютерных атак (КА), а простая комбинация разнообразных средств защиты приводит к снижению эффективности защиты в целом из-за конфликтности параметров разнородных средств защиты.Трудности определения оценок эффективности СЗИ связаны с несовершенством существующего нормативно-методического обеспечения информационной безопасности.

С целью решения указанной проблемы необходимо первоначально оценить эффективность каждого средства защиты ИТКС и разработать методику синтеза системы киберзащиты ИТКС.

В настоящее время разработана методика синтеза системы киберзащиты ИТКС и произведена оценка эффективности средств защиты при комплексном воздействии КА.

Для оценки эффективности средств защиты разработаны профильные модели процесса преодоления КА средств защиты и с помощью метода топологического преобразования стохастических сетей определено среднее время преодоления средств защиты каждой КА. На основании этих значений, как исходных данных, рассчитана вероятность предотвращения средствами защиты воздействия КА на ИТКС.

Используя полученные значения, как исходные данные, по разработанной методике обоснованы требования к средствам защиты и произведен синтез системы защиты ИТКС.

Анализ полученных результатов показал, что:

– средства защиты неэффективны при комплексном воздействии КА.

– средства защиты на элементах ИТКС должны размещаться комплексно. С целью снижения стоимости системы защиты все средства защиты должны быть универсальными, реализованными программно и установленными в элементы ИТКС еще на этапе их изготовления;

– для выполнения требований по защите ИТКС требуется увеличить частоту смены параметров средств защиты.

Заключение.

Высокие требования, предъявляемые к уровню защищенности информационно-телекоммуникационной сети (ИТКС), предопределяют необходимость проведения оценки эффективности системы защиты информации,

СПИСОКЛИТЕРАТУРЫ

1. Лаута О.С., Кузнецов С.И., Клиншов И.А., Смыгин А.М. Методика оценки компьютерных угроз на ИТКС. В сборнике: Радиолокация, навигация, связь Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1200.
2. Баранов В.В., Гудков М.А., Крибель А.М., Лаута О.С., Нечепуренко А.П. Защита канала управления роботизированных систем. В сборнике: Актуальные проблемы обеспечения информационной безопасности, труды Межвузовской научно-практической конференции. 2017. С. 32-37.
3. Баранов В.В., Крибель А.М., Лаута О.С., Нечепуренко А.П. Применение метода топологического преобразования стохастических сетей для оценки эффективности средств защиты.В сборнике: Актуальные проблемы обеспечения информационной безопасности, труды Межвузовской научно-практической конференции. 2017. С. 47-52.
4. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия. В сборнике: Радиолокация, навигация, связь Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 83-89.
5. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. Модель таргетированной кибернетической атаки. В сборнике: Радиолокация, навигация, связь Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 90-98.

УДК621.391(075.8)

ОБЕСПЕЧЕНИЕИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ ХРАНЕНИЯ ДАННЫХ

Ткаченко ВладимирВладиславович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail:U-429@inbox.ru

Аннотация. Проведен анализ реализуемых и перспективных подходов кприменению различных типов сетей хранения данных в интересах обеспечения информационной безопасности. Проанализированы вопросы информационной безопасности, требующие решения для сетей хранения данных.

Ключевые слова: *сеть хранения данных; информационная безопасность; цифровые ресурсы хранения; технологии.*

ENSURING INFORMATION SECURITY OF DATA STORAGE NETWORKS

Tkachenko Vladimir
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail:U-429@inbox.ru

Abstract. The analysis of implemented and perspective approaches to the applied types of networks data storage for the sake of information security. issues requiring data solutions for data protection.

Keywords: *storage system; information security; digital storage resources; technologies.*

Сегодня происходит радикальный сдвиг в технологиях в плане объемов данных, подлежащих управлению, и мест хранения этих ресурсов. Специалисты инженерно-технического профиля называют этот сдвиг взрывом данных [1]. И в то время как объемы информации растут в геометрической прогрессии, руководители компаний хотят добиться большей гибкости в обращении с данными, которая позволила бы им работать продуктивнее, быстрее и с большей экономией средств.

По мере роста требований к облачным ЦОД операторам центров предстоит решать нелегкую задачу: удерживать совокупную стоимость владения на низком уровне, сохраняя при этом высокие показатели производительности, надежности и безопасности.

Взрыв данных: определяющие факторы. Исследование компании Symantec выявило одну доминирующую тенденцию: коммерческие данные выходят за физические границы компаний и переходят в решения для облачного хранения. Согласно отчету, 20 % всех корпоративных данных в Северной Америке хранятся в облаке, а в некоторых странах этот показатель уже преодолел отметку в 30 %.

Запросы поставщиков видеосодержимого могут казаться уникальными, однако миграция видеофайлов в облако ставит задачи, схожие с теми, которые мы наблюдаем в развивающейся деловой экосистеме. По мере совершенствования технологий повышается качество видео, что приводит к росту емкостей хранения, необходимых для того, чтобы вместить все это содержимое. Это значит, что требования к решениям для основных хранилищ данных, резервного копирования, архивирования и аварийного восстановления значительно возрастают.

Системы хранения не являются изолированным элементом в ЦОД. Поэтому факторы, влияющие на оборудование хранилищ, влияют на безопасность всей остальной системы.

Потребители: персональные облачные системы хранения данных

Потребители оказывают значительное влияние на рост облачных СХД [2]. Согласно прогнозу Gartner, 46 % всего цифрового содержимого потребителей будет храниться к 2017г. в облаке. Кроме того, всемирный спрос на емкость существенно увеличился: от 329 экзабайт в 2011 г. до 4,1 зеттабайт в 2016 г.

Устройства с камерами, в частности смартфоны и планшетные ПК, пользуются все большей популярностью, и с их помощью создается все больший объем цифрового содержимого. Следовательно, растет и спрос на устройства хранения [3]. Gartner ожидает увеличения популярности поставщиков облачных СХД и служб синхронизации, как только спрос превысит возможности веб-сайтов социальных сетей, используемых в настоящее время для хранения большого объема цифрового содержимого.

Seagate заявляет, что даже с ростом общедоступных облачных СХД персональные облачные системы хранения данных в виде подключаемых напрямую и по сети домашних СХД составят значительную часть персональных облаков. Хранение 3,3 ТБ данных дома и еще некоторого их объема в общедоступной облачной СХД останется наиболее предпочтительным методом — в основном из соображений стоимости. Домашние системы NAS имеют много функций, наличествующих и в решениях NAS для малого бизнеса, благодаря чему с их помощью вполне реально создать персональную облачную СХД на несколько терабайт.

Требования к системам хранения довольно многоплановые —в особенности в потребительской сфере. Недостаточно предложить только дополнительные ресурсы для хранения, ведь ожидания в отношении производительности тоже растут. Как компании, так и отдельные пользователи нуждаются в платформах с высокой функциональной совместимостью, которые бы предоставляли возможность, к примеру, виртуализации и работы с большими данными независимо от инфраструктуры СХД [4].

В журнале TIME вышла статья под названием «Будущее персональных вычислений: повсеместное использование экранов, соединенных через облако», где превосходно описан рынок потребительских вычислений, движущийся в направлении персонализированных вычислений, при этом оговорено, что данная тенденция не ограничивается персональными облаками. Персонализированные вычисления пользуются все большей популярностью среди потребителей, компаний малого бизнеса и крупных предприятий. Облако играет исключительно важную роль для СХД будущего, в том смысле, что позволяет реализовать концепцию персонализированных вычислений. Однако это вовсе не означает конец эпохи традиционных систем хранения. Наоборот, с помощью облака пользователи смогут оптимизировать многие подключенные друг к другу решения для хранения данных в нашем заполненном информацией мире.

В связи с повсеместным и массовым использованием СХД возникают вопросы безопасности информационной составляющей СХД.

СПИСОК ЛИТЕРАТУРЫ

1. Спрос на устройства хранения в мире взаимосвязанных данных. // Seagate and BlackArmor, 2015. // [Электронный ресурс]: http://www.seagate.com/ru/ru/tech-insights/demand-for-storage.html.
2. Отчетмаркетинговогоподразделения Seagate и IDC Worldwide Enterprise Storage for Public and Private Cloud 2011-2015. // [Электронныйресурс]: http://www.idc.com/getdoc.jsp.containerId=230283.
3. Авраменко В.С. Адаптивный контроль защищенности информации от несанкционированного доступа на основе информационных образов. // Проблемы информационной безопасности. Компьютерные системы. 2010. № 2. С. 45-49.
4. Саенко И.Б., Бирюков М.А., Ефимов В.В., Ясинский С.А. Модель администрирования схем разграничения доступа в облачных инфраструктурах // Информация и космос. – 2017. – №1. – С. 121-126.

УДК 621.391(075.8)

БЕЗОПАСНОСТЬ В СЕТЯХ МОБИЛЬНОЙ СВЯЗИ. ЗАЩИТА ИНФОРМАЦИОННЫХ РЕСУРСОВ В СЕТЯХ 4G

Ульянов Максим Владимирович, Годунов Евгений Романович, Терехов Александр Геннадьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: max94-4@mail.ru

Аннотация. Предпринята попытка анализа безопасности, с точки зрения информационной безопасности, внедрения в нашу жизнь сетей LTE(4G).

Ключевые слова: *информационная безопасность; 4G; мобильная связь; LTE.*

SAFETY IN MOBILE COMMUNICATION NETWORKS PROTECTION OF INFORMATION RESOURCES IN NETWORKS 4G

Ulyanov Maxim, Godunov Evgenij, Terekhov Alexander
S.M. Budjonny Military Academy of the Signal Corps
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: max94-4@mail.ru

Abstract. An attempt was made to analyze security, from the point of view of information security, the introduction into our life of LTE (4G) networks.

Keywords: *Information Security; 4G; mobile connection; LTE.*

Представлены цели и задачи создания стандарта LTE. Проведен анализ основных качественных и количественных показателей сетей нового поколения и дан ответ на важный вопрос не превратятся ли мобильные сети в Интернет с присущими ему опасностями и проблемами? Развитее IT создает фундамент современной экономики государства и благосостояния ее людей. Без высокоскоростного мобильного интернета, доступного прямо здесь и сейчас, уже нельзя. Видеохостинги, потоковые сервисы воспроизведения музыки, общение по Skype или другому популярному мессенджеру с функцией видеозвонков всё это требует качественного высокоскоростного соединения. Поэтому целями создания стандарта LTE являются: увеличение возможностей высокоскоростных систем мобильной связи; уменьшение стоимости передачи данных; возможность предоставления широкого спектра недорогих услуг. Однако улучшение качественных и количественных показателей сетей нового поколения выдвигает и новые требования, связанные с повышением безопасности передаваемой информации. Поскольку технология 4G полностью основана на протоколе IP, не превратятся ли мобильные сети в Интернет с присущими ему опасностями и проблемами? Мобильная связь четвертого поколения предусматривает

использование целого спектра технологий, которые раньше развивались параллельно. Опора на множество различных технологий затрудняет поиск уязвимостей в LTE, что хорошо с точки зрения безопасности взлом радиоканала для одних методов может сработать, а для других нет. В сетях 4G весь трафик проходит через единую архитектуру по протоколу IP. Поэтому в компании Cisco считают, что все угрозы безопасности передаваемой информации связаны именно с протоколом IP. Базовые станции в LTE стали более интеллектуальными и самостоятельными они получили возможность маршрутизировать трафик, что позволило организовывать соединения между абонентами напрямую, минуя ядро сети. В результате у злоумышленников появилась возможность атаковать сами базовые станции, которые работают только по протоколу IP, поэтому облегчается несанкционированный доступ к сети и, следовательно, могут быть использованы классические атаки на канальном уровне, широковещательные штормы и другие варианты нападений. Чтобы свести к минимуму подверженность атакам конфиденциальную информацию, базовая станция должна обеспечить выполнение таких важных операций как кодирование и расшифровку пользователей данных, а также хранение ключей. Для минимизации вреда наносимого в случае кражи информации о ключах из базовых станций разработаны специальные меры противодействия: проверка целостности устройства; взаимная аутентификация базовой станции оператора (выдача сертификатов); безопасные обновления; механизм контроля доступа; синхронизация времени и фильтрация трафика [1].

Безопасность в сетях мобильной связи.

В настоящее время вирусы на компьютерах стали делом обычным, троянов для Android становится все больше, следовательно, внедрение высокоскоростного стандарта LTE приносит в мобильные средства связи все те угрозы, которые мы сейчас наблюдаем в ситуации с обычными компьютерами. Первая очевидная угроза атаки DoS на сеть (Denial of Service). Емкость радиоканала в LTE предполагается большая, но все, же она имеет ограничения. Сетевые ресурсы базовой станции делятся между абонентами, и, хотя есть ограничения для монополизации полосы отдельным пользователем, тем не менее, атака на отказ в обслуживании сети вполне возможна. Другая угроза Вирусные атаки. Хотя таким атакам подвержены устройства, а не сеть, технология LTE увеличивает скорость распространения вредоносных программ, поскольку сам этот стандарт является высокоскоростным. Третья опасность атаки на дополнительные сервисы, которые также могут быть уязвимы для самых разнообразных атак как из Интернета, так и из мобильной сети. Вполне возможно, что, атаковав один из сервисов, злоумышленники смогут внедрить в клиентские устройства опасные программы. Нельзя забьюать и об ограничениях LTE. Например, увеличение скорости подключения оборачивается обычно уменьшением радиуса действия базовой станции в среднем для 4G он составляет около 5 км, и зависит от используемого частотного диапазона. Поэтому базовых станций в сети становится больше, и они располагаются ближе друг к другу. В результате триангуляционный метод определения местоположения абонента по сигналам базовых станций работает точнее. С одной стороны, это можно использовать, например, для контроля за перемещением грузов и многого другого. Но с другой стороны, сервисы геопозиционирования (Locationbased service, LBS) можно использовать и для слежки за абонентом, что создает опасность новых угроз. Еще одна особенность LTE в том, что эта технология ориентирована на подключение интеллектуальных пользовательских устройств: компьютеров с LTE-модемами, планшетов или смартфонов. С их распространением число потенциально опасных сервисов будет только возрастать. Взлом такого сервиса позволит злоумышленникам получить доступ к ценной информации провайдера и построить новые схемы преступлений и незаконного получения денег.

Есть также проблемы и с самим стандартом. Очень остро стоит задача взаимодействия с недоверенными (не LTE) сетями. Если трафик между пользовательским оборудованием и базовой станцией шифруется (это требование стандарта) и угроза нарушения конфиденциальности становится неактуальной, то взаимодействие базовой станции с радиоконтроллером сети 3G по умолчанию никак не защищено, а, следовательно, это брешь для возможных атак со стороны злоумышленников. Другой проблемой является отсутствие обязательной аутентификации между ядром сети и базовой станцией. Эту опцию оператор связи для снижения своих издержек по развертыванию сети LTE может и не задействовать вовсе. И все же разработчики мобильной технологии LTE позаботились о ее защите несколько больше, чем разработчики Интернета [2]. Поэтому мобильная сеть является более надежной и безопасной, чем всемирная сеть так как, в основном, защита возложена на более интеллектуальные базовые станции. Все функции защиты в LTE объединены стандартом и подразумевают защиту на нескольких уровнях: на уровне доступа к сети; на уровнях сетевого и пользовательского доменов; на уровне приложений; на уровне отображения и конфигураций. Каждый из этих уровней предполагает аутентификацию и авторизацию всех устройств, чего нет в Интернете.

Кроме того, технология LTE предусматривает использование не только адреса, но и системы распространения ключей шифрования для всех устройств, подключенных к сети с возможностью перехода со 128 на 256 битные ключи и введения новых алгоритмов, сохраняя обратную

совместимость. Безопасность в сетях, мобильной связи. Помимо алгоритмов шифрования и обеспечения комплексной безопасности в сетях 4G используются дополнительные алгоритмы [3].

Таким образом, даже если один из алгоритмов будет взломан, оставшиеся обеспечат безопасность сети LTE. В сетях LTE сохраняются и методы аутентификации пользователей по привязке к SIM карте, как в традиционной мобильной связи. Пользователь может заблокировать доступ к телефону по PIN-коду.

СПИСОК ЛИТЕРАТУРЫ

1. Аналитический обзор защиты данных в сетях LTE. ПоматериаламNTTDOCOMOTechnicalJournalVol. 11 No. 3.http://advancedmonitoring. ru/article/detailphp 7ELEMENTJD-56 .
2. Баранов В.В., Бирюков М.А., Кравченко С.А., Максимов А.С., Саенко И.Б. Имитационная модель для анализа рисков информационной безопасности при проектировании ролевых схем разграничения доступа к базам данных // Актуальные проблемы обеспечения информационной безопасности. Труды межвузовской научно-практической конференции. 2017. С. 26-31.
3. LTE and the Evolution to 4G Wireless Design and Measurement C hallenges. Bonus Material: Security in the LTE-SAE Network, Agilent technologies 2010 p. 7.

УДК 621.391 (075.8)

К ВОПРОСУ О ПРОБЛЕМЕ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Усачев Игорь Владимирович, Кий Андрей Вячеславович, Зибров Олег Павлович,
Башкирцев Андрей Сергеевич, Щербаков Александр Юрьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: igus2@yandex.ru, kiyarmy@yandex.ru, ol.zibroff@yandex.ru, Ab098@yandex.ru

Аннотация. Проведен анализ проблемы защиты информации в автоматизированных системах специального назначения, выявлены задачи, решаемые системой защиты информации в процессе функционирования. В качестве совершенствования системы защиты информации предложена разработка методики по организации защиты информации в автоматизированных системах специального назначения.

Ключевые слова: *защита информации; автоматизированная система; несанкционированный доступ.*

TO THE QUESTION ABOUT THE PROBLEM OF INFORMATION SECURITY IN AUTOMATED SYSTEMS SPECIAL PURPOSE

Usachev Igor, Kiy Andrey, Zibrov Oleg, Bashkirtsev Andrey, Sherbakov Alexandr
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: igus2@yandex.ru; kiyarmy@yandex.ru; ol.zibroff@yandex.ru; Ab098@yandex.ru

Abstract. Theanalysis of the problems of information protection in automated systems for special purposes, the identified tasks of the security system during operation. The improvement of information security system is proposed to develop methods for the protection of information in automated systems for special purposes.

Key words:*information protection; automated system; unauthorized access.*

Современная тенденция развития разных сфер человеческой деятельности характеризуется высоким уровнем информатизации. Особое внимание уделяется объектам, на которых обрабатывается конфиденциальная информация. К таким объектам можно отнести автоматизированные системы специального назначения (АС СН) различных государственных структур, а также коммерческих организаций. Такие системы выполняют большое количество сложных задач, связанных с обработкой, хранением и передачей конфиденциальной информации.

В целях решения проблемы обеспечения безопасности информации в АС СН необходимо определить угрозы безопасности хранимой, обрабатываемой и передаваемой в ней информации. Возможности источников угроз безопасности информации обусловлены совокупностью способов несанкционированного и (или) случайного доступа к информации, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) информации.

К современным АС СН предъявляются высокие требования к безопасности информации, предполагающие их изоляцию от сетей общего пользования, либо применение криптотуннелей (при отсутствии такой возможности) [1, 2]. Основными структурными и функциональными особенностями современных АС СН являются следующие: многорежимность функционирования; высокий уровень оснащенности объектов автоматизации средствами вычислительной техники; значительное число пользователей и прикладных программ, имеющих непосредственный доступ к защищаемым

ресурсам; территориальная распределенность элементов АС СН; сосредоточение в отдельных элементах АС СН (серверах баз данных, серверах регламентной обработки данных и т.д.) значительных объемов информации различного назначения, принадлежности и грифа секретности; использование разнородных операционных систем отечественного и иностранного производства (Windows, аналогов Linux, FreeBSD и других).

Несмотря на огромные усилия как теоретического, так и практического характера, которые прикладываются к решению проблемы защиты информации в АС СН, состояние ее в настоящее время весьма далеко от надежного решения [3]. Более того, как показал многолетний опыт организации защиты информации в АС (в том числе и зарубежный), каким бы не был совершенным проект системы защиты и его первоначальная реализация, в процессе функционирования АС неизбежно возникают непредвиденные обстоятельства, обусловливаемые, как действиями факторов, неучтенных (или неадекватно учтенных) на этапе создания системы защиты, так и изменениями, происходящими в процессе функционирования АС. Например, возник ряд совершенно новых задач, связанных с проблемой компьютерных вирусов. В связи с этим неизбежно возникает необходимость совершенствования системы защиты информации [4].

Современные СЗИ от НСД в процессе своего функционирования решают множество задач, таких как:

– защита от вмешательства в процесс функционирования АС СН посторонних лиц (возможность использования АС СН и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

– разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам АС СН (обеспечение возможности доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям АС СН для выполнения ими своих служебных обязанностей);

– регистрацию действий пользователей при использовании защищаемых ресурсов АС СН в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов сотрудниками подразделений компьютерной безопасности;

– оперативный контроль за работой пользователей системы и оперативное оповещение администратора безопасности о попытках несанкционированного доступа к ресурсам системы;

– защиту от несанкционированной модификации (обеспечение неизменности, целостности) используемых в АС СН программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы и вредоносные «программы-закладки»;

– защиту хранимой, обрабатываемой и передаваемой по каналам связи информации ограниченного распространения от несанкционированного разглашения, искажения, подмены или фальсификации;

– управление информационными потоками между устройствами;

– обеспечение аутентификации абонентов, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

– гибкое управление всеми защитными механизмами

– мониторинг АС СН.

В связи с этим необходимо учитывать влияние функционирования СЗИ на работу АС СН по прямому назначению (обработка, хранение и передача конфиденциальной информации), связанное со значительным отвлечением вычислительных ресурсов АС СН, что отрицательно влияет на работоспособность системы в целом.

Достижение высокого уровня безопасности невозможно без принятия должных организационных мер, которые позволяют без значительных финансовых затрат эффективно разграничить доступ как к защищаемой информации, так и к самим объектам АС СН. С одной стороны, эти меры должны быть направлены на обеспечение правильности функционирования механизмов защиты, и предприниматься администратором безопасности системы. С другой стороны, руководство организации, эксплуатирующей средства автоматизации, должно регламентировать правила автоматизированной обработки информации, включая и правила ее защиты, а также установить степень ответственности за нарушение этих правил [4].

Основными направлениями организационных мер защиты информации являются: организация работы с персоналом; организация внутриобъектового и пропускного режимов и охраны; организация работы с носителями сведений, подлежащих защите; комплексное планирование мероприятий по защите информации; организация аналитической работы и контроля.

В качестве совершенствования СЗИ предлагается разработка методики по организации защиты информации, что позволит четко определить круг обязанностей по защите информации должностных лиц, повысить безопасность информации в АС СН, снизить издержки на обеспечение защиты информации в процессе функционирования АС СН и выполнении задач.

СПИСОК ЛИТЕРАТУРЫ

1. ФСТЭК РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. [Электронный ресурс]. — URL:

http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g
2. Брунилин А.А., Бирюков М.А., Саенко И.Б. Модель и метод использования онтологий для управления разграничением доступа в едином информационном пространстве // Математические методы в технике и технологиях – ММТТ. 2016. № 6 (88). С. 122-124.
3. Бирюков М.А. Разработка модели нарушителя правил разграничения доступа к единому информационному пространству // Математические методы в технике и технологиях – ММТТ. 2017. Т.3. С. 107-110.
4. Авраменко В.С. Способы идентификации нарушителя безопасности информации в автоматизированных системах на основе информационного почерка //В сборнике: Проблемы технического обеспечения войск в современных условиях. Труды II межвузовской научно-практической конференции. 2017. С. 36-40.

УДК: 004.41

ПРОГРАММНАЯ СИСТЕМА ДЛЯ МОНИТОРИНГА СЕТЕВОГО ОБОРУДОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Федосеев Денис Олегович, Корякин Денис Дмитриевич, Ястребов Егор Евгеньевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, пр. Тихорецкий,3
e-mail: yastrebov.ee@gmail.com

Аннотация. В работе приводится описание разрабатываемой системы мониторинга сетевого оборудования для контроля сети и обеспечения ее безопасности.

Ключевые слова: *информационная безопасность; мониторинг; сеть; программное обеспечение.*

NETWORK MONITORING SOFTWARE TO PROVIDE INFORMATION SECURITY

Fedoseev Denis, Koryakin Denis, Yastrebov Egor
S.M. Budjonny Military Academy of the Signal Corps,
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: *yastrebov.ee@gmail.com*

Abstract. The article describes the developing network monitoring system for control network equipment and ensuring information security.

Keywords: *information security; network; software; monitoring.*

Эволюционное развитие технологий, конкуренция производителей телекоммуникационного оборудования за преобладание на рынке, а также активно развивающееся в Российской Федерации импортозамещение в гражданской и особенно военной инфраструктуре приводят к тому, что инфраструктура сетей связи год за годом становится все более неоднородной[1]. Сеть организована при помощи оборудования, принадлежащего разным поколениям развития технологий и обладающего широким, почти нерегламентированным, набором функций, который поставляется различными производителями. За последние годы на действующих сетях связи успело накопиться аналоговое оборудование, цифровые станции и системы передачи, вслед за которыми пришли IP сети, мультимедийные и сигнальные шлюзы, Softswitch, SON (Self-organizing Networks)[2]. Мобильные технологии также не отстают, развиваясь от 3G до LTE, 5G и обновляя оборудование на более современное. Кроме совершенствования и появления новых видов технологий неоднородность сетей обуславливает использование несовместимого друг с другом оборудования всевозможных производителей. Каждый из них стремится заложить в свои продукты максимум различных функциональных возможностей, реализация которых, как правило, подразумевает использование нестандартных протоколов и специализированного программного обеспечения, разрабатываемого непосредственно вендором оборудования. В таких условиях оператору связи чрезвычайно трудно унифицировать взаимодействие с сетевым оборудованием и обеспечить управление всей сетью как одним целым. По этой причине могут возникать серьезные проблемы с информационной безопасностью в данных сетях. Особенно это прослеживается на стыке технологий.

Для подробного контроля сети и своевременного поиска несанкционированных изменений в конфигурации сетевых устройств разрабатывается решение, которое призвано обеспечить единый интерфейс взаимодействия со всеми сетевыми ресурсами вне зависимости от используемых технологий и оборудования. Это решение предоставит всем эксплуатационным службам достоверную и актуальную информацию о текущем состоянии и конфигурации сетевых ресурсов, а также о сохранности в сети.

Система призвана решить весь комплекс задач по взаимодействию с оборудованием: от проведения дистанционных измерений до удаленного конфигурирования и администрирования активных элементов в сети любого типа — от классических аналоговых и использующих TDM-технологии до IP оборудования последних поколений и сетей NGN. ПО позволяет инкапсулировать всю сложность и неоднородность технологических доменов используемого на сети оборудования от оператора автоматизированного рабочего места. Это свойство обеспечивает максимальную гибкость IT-инфраструктуры, позволяет

избавиться от необходимости постоянного обновления системы при появлении новых устройств с нестандартными протоколами взаимодействия.

В целом ПО предоставляет унифицированный интерфейс для любого оборудования в сети, что даёт следующие преимущества при использовании:

– скрывается технологическая разнородность сетей при помощи использования стандартных интерфейсов и/или протоколов и специально разработанных командных кодеков;

– предоставляется возможность взаимодействия с оконечным оборудованием пользователя по протоколу CWMP (TR-069);

– обеспечивается возможность конфигурации любого активного оборудования в рамках любого домена;

– обеспечивается сбор аварийной сигнализации, её фильтрация и представление в виде, удобном для дальнейшего анализа;

– обеспечивается возможность автоматического исследования сети.

Для того чтобы программное обеспечение предусматривало возможность динамически добавлять, изменять или удалять компоненты и кодеки для конкретных видов протоколов и устройств без необходимости переустановки и перезапуска системы используется модульная система – система плагинов. Для реализации такой возможности взята за основу существующая спецификация динамической модульной системы и сервисной платформы для Java-приложений – OSGi (Open Services Gateway Initiative)[3], для которой существуют несколько реализаций. Основные из них: Apache Felix, Spring DM (Dinamic Modules) и Gemini Blueprint, который является наследником Spring DM. Для применения в проекте предполагается использовать Spring DM или Gemini Blueprint, т.к. ядро системы разрабатывается с использованием Spring framework. Платформа OSGi позволяет управлять модулями, называемыми бандлами (bandle). Каждый бандл – логически завершенный программный компонент, который реализует определенный функционал.

Она состоит из следующих модулей:

– Модуль, отвечающий за пользовательский интерфейс;

– Модуль взаимодействия с хранилищем (базой данных);

– Модуль взаимодействия с оборудованием, который включает в себя подмодули для взаимодействия с конкретными протоколами, к примеру, SNMP[4], Telnet и SSH, а также конкретными устройствами;

– Модуль построения топологии (карты) существующей сети;

– Модуль для предоставления API для мобильного приложения для экстренного оповещения.

Пользователь может взаимодействовать с системой несколькими способами: с автоматизированного рабочего места, которым является любой ПК, подключенный к сети, где запущена система посредством веб-браузера, мобильного телефона или планшета. Мобильные клиенты позволяют своевременно получать уведомления о нарушениях работы в сети, ее взломах, несанкционированном доступе к устройствам и возможной утери информации.

Также в самой системе реализуется подсистема авторизации и аутентификации пользователей, чтобы запретить доступ к системе неавторизированным пользователям, а также ограничить доступ к определенным страницам и функциям. Это необходимо для четкого разделения пользователей по их квалификации, например, оператор АРМ, администратор системы. Реализация подобного функционала в системе позволяет увеличить безопасность хранимых данных и избежать утечек, а также проследить действия каждого пользователя в системе в соответствии с его полномочиями. Оператор АРМ должен иметь доступ только к просмотру сведений о сети: карты сети, состояниях устройств и т.п., а администратор системы должен иметь возможность заходить на страницы настроек, должен иметь возможность добавлять и настраивать устройства в системе. Также можно выделить в отдельную роль добавление и редактирование модулей, плагинов в системе.

Задача мониторинга сети в настоящее время является актуальной, поэтому разработка универсальной системы, которая позволяет производить диагностику объектов в сети, скрывая от пользователя сложность технологических доменов? является важной и перспективной задачей. Также универсальный метод получения измерений и данных о состоянии сети и устройств в ней применим для автоматизированного вмешательства для поддержки качества предоставления связи и обеспечения безопасности коммуникаций.

СПИСОК ЛИТЕРАТУРЫ

1. Ермишян А.Г. Теоретические основы построения систем военной связи в объединениях и соединениях. Ч. 1. – СПб.: ВАС, 2005, с. 740.
2. Гольдштейн А.Б. Устройства управления мультисервисными сетями: Softswitch (Статья) // Журнал «Вестник связи». - М., 2002. - №4
3. Бирюков М.А. Разработка модели нарушителя правил разграничения доступа к единому информационному пространству // Математические методы в технике и технологиях – ММТТ. 2017. Т. 3. С. 107-110.
4. Агеев С.А., Шерстюк Ю.М., Саенко И.Б., Полубелова О.В. Концептуальные основы автоматизации управления защищенными мультисервисными сетями // Проблемы информационной безопасности. Компьютерные системы. 2011. № 3 С. 30-39.

УДК 004.056.53

МЕТОДИКА ПРОЕКТИРОВАНИЯ СИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Фиалкин Илья Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail:ifialkin-81@mail.ru

Аннотация. В докладе рассмотрены актуальные вопросы защиты информации от несанкционированного доступа в автоматизированных информационных системах, формирования предложения по совершенствованию подсистемы управления доступом, как основы системы защиты информации. Предлагается методика проектирования системы разграничения на основе функционально-ролевой модели.

Ключевые слова: *разграничение доступа; информационные ресурсы; защита информации; функционально-ролевая модель.*

THE DESIGN METHOD OF SYSTEM ACCESS SECURITYAUTOMATED INFORMATION SYSTEMS

Fialkin Ilya
Military Academy of communications
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: ifialkin-81@mail.ru

Abstract. The article deals with relevant questions of information protection from unauthorized access in automated information systems, the formation of proposals to improve the access management subsystem, as the basis for the information security system. A method of designing control system based on the functional-role models.

Keywords: *access control; information resources; information security; functional-role model.*

Базовым элементом современных систем защиты информации является система разграничения доступа к информационным ресурсам системы. В соответствии с требованиями приказов (стандартов) в области информационной безопасности система разграничения доступа должна строиться на основе формальных моделей разграничения доступа. Данные модели строго определяют свойства элементов системы, правила их взаимодействия и позволяют проводить математическое доказательство безопасности системы. Однако, наличие формальной модели безопасности не является достаточным условием для построения гарантированно защищенной системы [1]. Необходимо обеспечить полное соответствие абстрактных сущностей и процессов модели реальным объектам и правилам функционирования системы.

Поэтому большую роль при построении систем защиты информации и разграничения доступа играют методики, позволяющие с высокой степенью адекватности интерпретировать формальную модель безопасности в реальной системе. Однако при разработке и применении подобных методик возникают сложности, связанные с особенностями современных информационных систем (ИС). К ним относятся разветвленная организационно-штатная структура, различные классы информационных ресурсов и процессов их обработки, специфика предметной области ИС и многое другое.

Из всего комплекса задач и элементов проектирования автоматизированных информационных систем (АИС), необходимых для создания системы разграничения доступа, выделим формирование структуры информационных ресурсов, разработку функционально-алгоритмической структуры, построение системы ролей и рабочих групп пользователей, что формирует исходные условия создания системы разграничения доступа согласно функционально-ролевой модели безопасности АИС. Решение данных задач должно быть основано на детальном анализе предметной области АИС, среди которых организационно-штатная структура, функциональная модель деятельности, модели процессов и потоков данных, формируемых в рамках проектирования АИС.

Таким образом, методика построения системы разграничения доступа должна содержать следующие этапы [2]:

– построение структуры информационных ресурсов системы;

– определение набора процессов и процедур для формирования функциональных модулей, т.е. построение функционально-алгоритмической структуры системы;

– создание ролей, групп на основе функциональных обязанностей персонала и организационно-штатной структуры;

– назначение итоговых (ролевых и индивидуальных) прав доступа.

После построения системы разграничения доступа необходимо провести оценку эффективности системы согласно критерию эффективности и на основе результатов оценки принять решение либо о достижении цели построения системы, либо о корректировке элементов системы.

Проектирование системы разграничения доступа – многокритериальная задача. В общем случае система критериев, используемых при планировании системы, имеет иерархическую структуру. Центральной проблемой разработки распределенных процедур решения сложных задач является нахождение такой декомпозиции распределения на подзадачи, а также выбор таких методов решения в каждом элементе созданной структуры, которые приводили бы к получению приемлемого по качеству решения всей задачи в целом за приемлемое время [3].

В основе декомпозиционного подхода лежит предположение о наличии общей глобальной модели информационной защиты, которая описывает основные свойства системы адекватно поставленным целям принятия решения. При наличии такой модели применение декомпозиционых методов позволяет резко сократить размерность решаемой задачи и свести ее к последовательному решению ряда задач намного меньшей размерности. Все модели, ограничения и критерии этих задач непосредственно вытекают только из специальным образом расчлененной глобальной целевой функции. При декомпозиционном подходе алгоритм взаимодействия между подсистемами (решаемыми задачами) [4] и характер потоков информации между вышестоящими и нижестоящими уровнями являются производными и определяются методом декомпозиции глобальной задачи.

Попытка непосредственного использования единого глобального критерия верхнего уровня с последующей его декомпозицией для подсистем всех уровней делает задачу оптимизации крайне сложной и игнорирует наличие собственных целевых функций у активных подсистем. Оптимальное решение многоуровневой иерархической системы обладает тем свойством, что каковы бы ни были состояние и решение вышестоящего уровня управления в момент t, последующие решения нижестоящих уровней должны быть оптимальными относительно этого решения.

Применение принципа оптимальности позволяет реализовать наиболее эффективный способ координации решений, принимаемых на отдельных уровнях иерархии. Этот принцип позволяет до минимума сократить обмен информацией между уровнями и обеспечить локальную обработку информации по подсистемам [5].Поэтому необходимо проводить оценку выполнения поставленных требований на каждом этапе построения системы разграничения доступа, при этом критерии оптимальности каждого из этапов должны быть связаны с критерием оптимальности всей системы.

В связи с этим расширим методику за счет добавления процедур оценки эффективности каждого из этапов и процедуры итоговой оценки эффективности системы в целом. При этом по итогам оценки эффективности этапа возможна корректировка полученных результатов в случае, если не были достигнуты требуемые характеристики. Особую роль в методике играет процедура итоговой оценки эффективности системы, результат которой определяет степень удовлетворения построенной системы основному критерию проектируемой системы разграничения доступа. На основе данного результата корректировке может быть подвергнута любая из подсистем, построенных на предыдущих этапах.

СПИСОК ЛИТЕРАТУРЫ

1. Будко Н.П., Будко П.А., Булгаков О.Ю., Васильев В.В., Давидчук В.В., Евграфов А.Е., Жук А.П., Карпов В.В., Князев В.В., Лепешкин О.М. и др.Интеллектуализация сложных систем язык схем радикалов в проблемных вопросах предпроектных исследований, оснащения, сопровождения систем и в экспериментальных задачах внедрения критических наукоемких технологий. - Информационно-измерительные и управляющие системы. 2009. Т. 7. № 3. С. 1-92.М.: Яхтсмен, 1996. - 192 с.
2. Краснокутский А.В., Лепешкин О.М., Харечкин П.В. Анализ функциональной применимости ролевой модели разграничения доступа в системах управления. Инфокоммуникационные технологии. 2007. Т. 5. № 3. С. 162-164.
3. Лепешкин О.М., Харечкин П.В. Функционально-ролевая модель управление доступом в социотехнических системах. Известия ЮФУ. Технические науки. 2009. № 11 (100). С. 52-57.
4. Лепешкин О.М. Методика реализации функционально-дискреционной модели на основе среды радикалов. Известия ЮФУ. Технические науки. 2009. № 11 (100). С. 21-26.
5. Лепешкин О.М., Харечкин П.В. Подходы к обеспечению функциональной применимости ролевой модели разграничение доступа в системе управления предприятия. Информационное противодействие угрозам терроризма. 2008. № 11. С. 57-66.

УДК 004.021

АНАЛИЗ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ХЕШ-ФУНКЦИЙ ДЛЯ СРАВНЕНИЯ ТЕКСТОВ БЕЗ РАСКРЫТИЯ СОДЕРЖИМОГО

Хилько Валерий Олегович, Левкин Александр Сергеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail:eaklone@yandex.ru

Аннотация. Рассмотрен метод использования существующих криптографических и не криптографических хеш-функций при защищенном хранении и анализе текстов, преимущества и недостатки данного подхода, а также выдвинуты предположения в отношении наиболее подходящих хеш-функции, применяемых для этой цели.

Ключевые слова: *хеш-функции; информационная безопасность; анализ текста; поиск.*

ANALYSIS OF POSSIBILITIES USING A HASH FUNCTION FOR TEXT COMPARISON WITHOUT OPENING THE CONTENTS

Khilko Valeriy, Levkin Aleksandr
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail:eaklone@yandex.ru

Abstract. The paper describes the method of using the existing cryptographic and cryptographic hash functions for secure storage and analysis of the texts, the advantages and disadvantages of this approach and put forward suggestions on the most appropriate hash function used for this purpose.

Keywords: *hash functions; information security; text analysis; search.*

При хранении текста, содержащего сведения, предназначенные для определенного круга лиц, в электронном виде неизбежно возникает проблема защиты его от несанкционированного доступа, так как нет гарантии того, что к текстам не получат доступ лица, не имеющие на это прав. В определенных областях такой подход является вынужденной мерой, однако, при их хранении без необходимости непосредственного взаимодействия с текстом появляется возможность хранить не сам текст, а лишь какую-нибудь его характеристику, позволяющую совершать все необходимые действия. При этом в отдельных случаях можно (и даже необходимо) преобразовать текст так, чтобы исключить возможность его обратного преобразования для получения информации.

В этом случае хеш-функция представляет собой весьма интересный инструмент, так как она с очень высокой вероятностью возвращает уникальные значения для разных текстов, что позволяет использовать ее в качестве характеристики текстов. В то же время процесс обратного ее вычисления представляет собой очень сложную задачу (в случаях со специальными криптографическими хеш-функциями практически нереализуемую).

Рассмотрим, например, алгоритм CRC 32 с порождающим полиномом CRC-32-IEEE 802.3, он даст число возможных вариантов хеш-сумм 232. Вероятность же обратного вычисления ничтожно мала, так как основной метод обратного преобразования – сравнение по «радужным таблицам», хранящим наборы сопоставленных между собой пар хеш-сумма – текст. То есть, для того, чтобы получить исходное значение преобразованного текста, он должен быть уже известен, а в этом случае не было бы необходимости его обратного преобразования.

Быстродействие этого способа также достаточно велико, так как для добавления документа необходимо один раз преобразовать текстовый документ, после чего значение его хеш-суммы добавляется в базу данных. Однако, данный метод, реализуя невозможность получения доступа к исходному тексту, одновременно не дает возможности изменить текст, занесенный в базу данных после преобразования, так что после каждого изменения исходного текста необходимо заново заносить его в общую базу.

Для сравнения документов между собой можно воспользоваться так называемым алгоритмом шинглов, при котором производится удаление из текста всех служебных символов, предлогов, союзов и т.д., разбиение его на отдельные последовательности слов, начиная с первого, со смещением на одно слово за раз, вычисление хеш-сумм от каждой из них. Документ хранится в виде набора хеш-сумм, что полностью исключает возможность его прочтения. Сравниваются лишь хеш-суммы последовательностей слов документов. При использовании не криптографических хеш-функций и большого числа текстовой информации, согласно принципу Дирихле, неизбежно возникновение коллизий (одинаковых значений хеш-сумм, полученных от разных текстовых последовательностей). Этот факт вносит небольшую погрешность при сравнении, не играющую большой роли, так как число хеш-сумм для одного текстового документа, содержащего 2000 слов, делящегося по 5 слов при смещении на 1 слово за раз, составит 1996.

Перевод текстовых блоков в их контрольные суммы особенно привлекателен тем, что не только ускоряет процесс сравнения, создавая хеш-таблицы, но и предоставляет возможность использовать хеш-функции с гарантированной невозможностью обратного вычисления исходного текста (например, стандарты SHA-2, ГОСТ 34.11-94). Помимо этого, становится возможным хранить базу преобразованных для сравнения текстов без возможности их прочтения, что позволяет, используя доверенные криптоалгоритмы, обрабатывать сведения, составляющие государственную тайну.

Однако, применение криптографических хеш-функций с величиной хеш-суммы 128 бит и более связано со значительным временем обработки текстового документа, помимо этого длина хеш-суммы становится сопоставима с длинной входного сообщения, что существенно снижает перспективы применения хеш-функции для хранения текстового документа.

Таким образом, целесообразно использовать не криптографические хеш-функции с длинной хеш-суммы до 64 бит, так как они показывают наибольшее быстродействие при хешировании небольших строк. Число коллизий в случае использования хеш-функций с длинами хеш-сумм 32-64 бита не оказывает существенного влияния на конечную цель преобразования документа, так как

отношение числа коллизий к общему числу хеш-сумм, которыми характеризуется документ, пренебрежительно мало.

В представленной работе рассмотрен метод хранения текстовых данных для их сравнения, исключающий доступ к текстовой информации. Дальнейшей задачей является поиск наиболее подходящей хеш-функции, обеспечивающей наибольшее быстродействие, а также обоснование гарантированной невозможности ее обратного вычисления.

СПИСОК ЛИТЕРАТУРЫ

1. RossN. Williams Элементарное руководство по CRC алгоритмам обнаружения ошибок. : Rocksoft Pty Ltd., 1997, 376с.
2. Ландэ Д.В., Снарский А.А., Безсуднов А.В. Интернетика. Навигация в сложных сетях. Модели и алгоритмы. М.: Либроком, 2009, 295 с.
3. Зеленков Ю.Г., Сегалович И.В. Сравнительный анализ методов определения нечетких дубликатов для Web-документов // Труды 9 ой Всероссийской научной конференции «Электронные библиотеки: перспективные методы и технологии, электронные коллекции». RCDL'2007, Переславль, Россия, 2007. –Том 1, С. 166-174.

УДК621.391(075.8)

ПОИСК ДУБЛИКАТОВ В ИСХОДНЫХ КОДАХ ПРОГРАММ

Хилько Валерий Олегович, Шаров Илья Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mails: valebob@mail.ru, sharovilya27@yandex.ru

Аннотация. В докладе рассматривается подход, основанный на методе токенизации и алгоритме нахождения наибольшей общей последовательности для обнаружения дублирующих фрагментов кода в студенческих работах. Даются общие рекомендации по использованию метода токенизации.

Ключевые слова: *плагиат в исходных кодах; метод токенизации.*

SEARCH FOR COPIES IN SOURCE CODE

Khilko Valery, Sharov Ilya
Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mails: valebob@mail.ru, sharovilya27@yandex.ru

Abstract. The paper deals with the approach based on the tokenization method and the algorithm for finding the largest common sequence for detecting duplicate code fragments in student works. General recommendations are given on the use of the tokenization method.

Keywords*: source-code plagiarism; token-based approach.*

Студенты большинства ВУЗов страны очень часто используют в своих работах материал, который был создан не ими, что называется плагиат. При этом сами они, получив легкую оценку, не понимают, что, используя чужие знания, они наносят ущерб своим собственным, и причиняют вред всему дальнейшему процессу их обучения. Можно смело сделать заявление, что если студент не усвоит курс программирования еще на самых первых этапах обучения, то в дальнейшем он не будет успевать по дисциплинам соответствующего направления. Помимо того, что студенты не понимают, как важно самостоятельно выполнять заданные им работы, они занимаются плагиатом и по ряду других причин, таких как: отсутствие у них мотивации к самостоятельному изучению программы, недостаток времени, нехватка теоретических знаний, что ведет к отсутствию практических умений, а также совместная работа над заданием, когда задачи распределены неравномерно. Использование плагиата в дальнейшем влечет за собой повторное регистрирование кода, что сегодня является очень крупной проблемой. Все это, начинаясь с, казалось бы, несерьезных нарушений в виде получения незаслуженной оценки, впоследствии выходит на более серьезный уровень, где за подобное можно получить обвинение в нарушении авторских прав.

Создание подобной системы вызвано несколькими причинами:

– не существует такой базы, в которой хранилась бы информация обо всех работах, которые прошли проверку;

– детекторы, которые разработаны на сегодняшний день, поддерживают не все языки программирования;

– отсутствие такого клиента, с помощью которого преподаватели и студенты могли бы загружать работы и получать соответствующие результаты проверки.

Реализовывать детектор было решено с помощью метода токенизации. Его основу составляет получение соответствий инициализаций и объявлений, операторов и служебных слов с символами или их наборами, а также приведение всевозможный языков программирования к общему формату.

Алгоритм поиска заимствований необходимо построить с использованием следующих этапов, которые в общем случае проходит программа, когда ищет совпадения:

– этап подготовки – удаление лишних элементов кода, а именно пробелов, комментариев и последовательностей операторов, которые не имеет смысла рассматривать (например, код, который написан по определенному шаблону, известному еще до выполнения работы);

– этап преобразований – на этом этапе код, прошедший первый этап преобразовывается в тот формат, который необходим для использования выбранного метода (в данном случае выделяются токены);

– этап обнаружения совпадений – по тексту, который был преобразован, производится поиск дублирующих фрагментов;

– этап форматирования – составление соответствий между оригинальными фрагментами кода и найденными совпадениями в последовательностях токенов;

– этап представления сведений о проверке – представляется результат проверки, производится вывод отношения количества дублирующих элементов кода проверяемой программы из всех файлов, которые находятся в базе, к количеству всех элементов в процентном соотношении;

На сегодняшний день плагиат, который может быть использован в кодах работ студентов, остается серьезной проблемой во всех образовательных учреждениях не только России, но других стран мира. Во многих ведущих институтах используются детекторы плагиата. Наиболее известные среди них: Калифорнийский университет в Беркли, Стэндфордский университет и Массачусетский Технологический Институт. При борьбе с плагиатом необходимо помнить, что не нужно полагаться исключительно на детектор плагиата, важно также объяснять студентам возможные последствия использования не своих работ, повышая тем самым их персональную ответственность.

Планы на будущее по разработке системы поиска дублирующих элементов в исходном коде программы, отправленной на проверку, заключаются в следующем: создание удобного и понятного на интуитивном уровне интерфейса программы-клиента, создание общей базы соответствий служебных слов всевозможных языков программирования и токенов, а также создание нового метода, который позволит наиболее эффективно находить процент совпадений материала в двух файлах.

СПИСОК ЛИТЕРАТУРЫ

1. Лифшиц Ю., Антипов Д., Ефтифеева О., Котов А., Красс А., Лакунин М., Лысенко Е., Семенников А., Счастливцев Р. Обзор автоматических детекторов плагиата в программах.
2. Программа обнаружения плагиата в программных текстах MOSS [Офиц. сайт]. URL: http://theory.stanford.edu/~aiken/moss/
3. Коэффициент Жаккара [Электронный ресурс] // Свободная электронная энциклопедия [Офиц. сайт]. URL: http://en.wikipedia.org/wiki/Jaccard_index
4. Проблема поиска наибольшей общей подстроки [Электронный ресурс] // Свободная электронная энциклопедия [Офиц. сайт]. URL: http://en.wikipedia.org/wiki/Longest_common_substring_problem (дата обращения: 01.02.2014)
5. Программа поиска дублирующих фрагментов кода JPlag [Офиц. сайт]. URL: https://jplag.ipd.kit.edu/

УДК 004.056.53

МОДЕЛЬ ДЛЯ ОПРЕДЕЛЕНИЯ СКРЫТНОСТИ СИСТЕМЫ СВЯЗИ

Худайназаров Юрий Кахрамонович, Маслов Олег Николаевич, Барауля Игорь Геннадьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail:nastia-petror@mail.ru

Аннотация. В докладе рассмотрен процесс обратного преобразование «эфирных образов» в реальные объекты, отображающие пространство этих сигналов в деятельность сил, а также модель для определения скрытности формируемой системы связи.

Ключевые слова: *подсистема добывания; подсистемой обработки; радиосвязь; эфирный образ, информационная структура, процесс управления.*

A MODEL FOR DETERMINATION OF SECRECY COMMUNICATION SYSTEM

Hudaynazarov Yuri**,** Maslov Oleg, Baraulya Igor
Military Academy of communications
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail:nastia-petror@mail.ru

Abstract. The report describes the process of reverse transformation of the "essential image" in the real objects that show the space of these signals in the activity and also forces the model to determine generated stealth communication system.

Keywords: *the extraction subsystem; a subsystem of processing; telecommunication; ethereal image, information structure, process management.*

Современные операции отличаются высокой мобильностью. Высокая мобильность приводит к тому, что основным средством управления становятся различные виды радиосвязи. Высокая

насыщенность радиоэлектронными средствами и необходимость их постоянной или периодической работы на излучение приводят к тому, что деятельность войск (сил) с их помощью отображается в пространство сигналов радиоэлектронных средств, формируя там «эфирные» объекты - образы реальных физических объектов и связей между ними, имеющих определенную степень сходства с реальными объектами и их взаимосвязями.

Принимая во внимание тот факт, что система связи является динамически изменяющимся объектом, подверженным различным и трудно прогнозируемым видам воздействий противника, в этих условиях актуальным становиться вопрос моделирования поведения системы связи с учетом обеспечения ее скрытности [1].

Так, радиосвязь, обеспечивая управление силами, отображает в пространство сигналов радиосвязи структуру системы связи, процессы управления, отражающие деятельность сил. Таким образом, система связи является постоянным, непрерывным, глобальным источником информации о деятельности сил, перекрыть который можно, лишь прекратив связь, что ведет к потере управления. В свою очередь средства радиоэлектронной разведки (РЭР), наблюдая за пространством сигналов радиоэлектронных средств, производят обратное преобразование «эфирных образов» в реальные объекты, т.е. отображают пространство этих сигналов в деятельность сил [2].

Процесс обратного преобразования состоит из двух этапов, реализуемых соответственно двумя подсистемами радиоразведки - подсистемой добывания и подсистемой обработки. Эффективность подсистемы добывания характеризуется вероятностями обнаружения, распознавания (анализа), определения местоположения источника излучений (пеленгования), перехвата сообщения. Этими же вероятностями характеризуется скрытность объектов (источников сигналов).

Подсистема обработки на основе анализа данных, полученных подсистемой добывания, может дать с высокой вероятностью заключение о составе сил, их боевой организации, оперативном построении, о характере, порядке и последовательности выполняемых задач силами, т.е. о замысле применения сил. Таким образом, используя современные методы обработки, РЭР противника может проникать в планы и замыслы, не раскрывая содержания сообщений, передаваемых по каналам связи.

Например, экспертная система HANNIBAL - интерпретатор радиообмена - предназначена, по заявлению ее авторов, «для выдачи командиру на поле боя рекомендаций по оперативному построению и замыслу применения сил (войск) по результатам перехвата радиообмена». Показателем эффективности такой системы является вероятность правильного распознавания по работе связи к заданному времени замысла применения сил противника. Более поздней разработкой, построенной на принципах экспертных систем, стала ASAS - система автоматизированной обработки разведывательной информации от всех источников (all source automatic system), принятая на вооружение в странах НАТО в начале 90-х годов. Показателем эффективности такой системы реально может быть вероятность правильного распознавания замысла применения сил на основе информации от всех источников.

Для формализации деятельности сил разработан метод системного представления деятельности сил. Сущность его заключается в том, что для описания деятельности сил используют набор структур, отражающих основные аспекты деятельности сил, информационную структуру, отображающую каналы связи между пунктами и объектами управления.

Этот набор структур является необходимым и достаточным для того, чтобы однозначно представлять деятельность сил (задачи, замысел, решение, план). Так, боевая организация, количественный и качественный состав группировок сил задается составом и организационной структурой; оперативное построение и боевые порядки - пространственной структурой; задачи, порядок и последовательность их выполнения - временной структурой; организация управления, взаимодействия и связи- информационной структурой.

Все рассмотренные структуры при описании деятельности сил представляются детерминированными взвешенными графами и являются эталонами вариантов деятельности сил, замысла их применения, задач, решаемых силами. Накопление и систематизация таких эталонов являются основной задачей разведки противника в мирное время, поскольку в ходе боевой и оперативной подготовки отрабатывается то, что нужно на войне. Эти же структуры служат и для описания системных демаскирующих признаков при распознавании характера деятельности сил разведкой противника. Математически они также представляются взвешенными графами, только вероятностными. В качестве весов используются накопленные к заданному времени вероятности обнаружения, распознавания, пеленгования и перехвата излучений, зависящие от текущею времени, интенсивности излучений и характеристик подсистемы добывания по единичным излучениям [3, 4].

Вычисление накопленных вероятностей по указанным исходным данным соответствует процессу отображения деятельности сил в пространство сигналов радиосвязи к заданному моменту. Процесс обратного преобразования отображения пространства сигналов в предметную область, т.е. превращение «эфирных образов» и их связей в реальные взаимосвязанные объекты, описывается статистическим розыгрышем накопленных вероятностей, которые дают конкретные реализации

структур, соответствующих своим или другим (ложным) структурам эталонов. Сравнение структур-реализаций со структурами талонами осуществляется в виде операции распознавания изоморфности (изоморфного вложения) графов реализаций и графов эталонов. Решение о принадлежности варианта реализации к одному из вариантов эталона принимается по критерию минимума меры различии по совокупности структур.

Результатом моделирования является получение статистических оценок, т.е. отношения числа Mj/k принятых решении отнесения варианта реализации к i-му эталону (при фактическом исполнении варианта k) к общему числу реализации (N) и данном временном сечении (t). При i=k это решение является показателем скрытности связи (точнее, ее нескрытности), а при i≠k - показателем эффективности оперативной радиомаскировки, т.е. вероятностью навязывания радиоразведке противника средствами связи i-го ложного варианта замысла при фактической реализации k-го варианта.

При моделировании в качестве основных видов разведок, действующих против элементов системы связи необходимо учитывать радиолокационную, инфракрасную, радиоразведку и техническую компьютерную разведку. В качестве прогнозируемых внешних деструктивных воздействий на систему связи в модели целесообразно учитывать огневое поражение и воздействия электромагнитной энергией высокого уровня и особенно дистанционные программные воздействия. В качестве наиболее актуального на сегодняшний день воздействия, как в угрожаемый период, так и военное время [5].

Заключение. Предложенная модель может использоваться в учебном процессе высших военных учебных заведениях, при исследовании вопросов организации связи в ходе проведения современных операций, а также различными должностными лицами органов военного управления на этапах планирования и функционирования системы связи.

СПИСОК ЛИТЕРАТУРЫ

1. Каневский З.М., Литвиненко В.П., Макаров Г.В. Теория скрытности. Часть 1, Основы теории скрытности: Учеб. пособие. Воронеж: Воронеж. гос. техн. ун-т, 2003. 92 с.
2. Литвиненко В.П. Основы теории скрытности: практикум: учеб. пособие / В.П. Литвиненко. Воронеж: ГОУВПО «Воронежский государственный технический университет», 2010. 106 с.
3. Лепешкин О.М. Исследование функциональной безопасности систем государственного управления. Инфокоммуникационные технологии. 2007. Т. 5. № 3. С. 165-166.
4. Лепешкин О.М., Корсунский А.С. Оптимизация структуры комплекса информационно-технических средств в автоматизированных системах управления. Автоматизация процессов управления. 2011. № 4. С. 76-81.
5. Лепешкин О.М., Харечкин П.В. Управление конфликтным процессом решения коллективной задачи социотехнической информационной системы в условиях ресурсной координации. Информационное противодействие угрозам терроризма. 2010. № 14. С. 162-166.

УДК 681.322

НЕОБХОДИМОСТЬ РАЗРАБОТКИ СИСТЕМЫ ТРЕБОВАНИЙ К ОПЕРАЦИОННЫМ СИСТЕМАМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Чесноков Александр Валерьевич, Юдин Анатолий Алексеевич, Алексеев Олег Владимирович
Военная академия связи имени Маршала Советского Союза С.М. Будённого
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: garlic.a@yandex.ru

Аннотация. В докладе рассмотрены вопросы импортозамещения, в которых предусматривается замена в муниципалитетах России операционных систем MSWindows на системы с открытым исходным кодом, разрабатываемые российскими компаниями и дальнейшего развития российской индустрии в области информационных технологий.

Ключевые слова: *операционная система; windows; linux.*

THE NEED FOR THE DEVELOPMENT OF THE SYSTEM REQUIREMENTS OPERATING SYSTEMS OF SPECIAL PURPOSE

Chesnokov Alexander, Yudin Anatoly, Alekseev Oleg
Military academy of telecommunications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tikhoretskiy pr., 3,
e-mail: garlic.a@yandex.ru

Abstract. In the report are considered the issues of import substitution, which called for replacing the Russian municipalities of the MS Windows operating systems from Microsoft to the open source code developed by Russian companies and the further development of Russian industry in the field of information technology.

Keywords: *operating system; windows; linux.*

В настоящее время, с целью обеспечения безопасности и надёжной защиты информации от несанкционированного доступа, уделяется большое внимание разработке, и использованию во всех Федеральных службах и Министерствах Российской Федерации отечественной продукции (в нашем случае уделим внимание операционным системам).

Такие значимые организации, обеспечивающие безопасную жизнь всего государства, не должны использовать комплексы программ для управления ресурсами (операционные системы) иностранной разработки с закрытым кодом.

На данный момент ситуация с операционными системами довольно сложна с точки зрения затрат на конкуренцию с MS Windows. Затраты настолько велики, что большинство разработчиков на это серьёзным образом не рассчитывают. Все проекты, ориентированы на те или иные применения. Например, некоторые операционные системы адресованы проектам, где требуется высокая надёжность и скорость перезапуска аппаратуры (такие необходимы в области применения беспилотных летательных аппаратов).

Обратившись к ресурсу – «Реестр федеральных государственных информационных систем», можно наглядно увидеть в какой степени используются те, или иные операционные системы в государственных структурах (не являющиеся секретными).

Вот так, примерно, обстоят дела в настоящее время:

По поддерживаем серверным операционным системам, на первом месте находится MS Windows, далее Linux и Solaris (из отечественных разработок также упоминается МСВС).

Распределение мест по поддерживаемым клиентским операционным системам: первое у MS Windows; второе занимает Linux, на третьем - Mac OS.

По использованию офисного программного обеспечения, большим спросом пользуется Microsoft Office и Open/Libre Office.

Из этого следует, что MS Windows все же, является наиболее популярной операционной системой. Главная проблема внедрения Linux-подобных систем в том, чтобы они поддерживали работу специальных программ, которые установлены на компьютерах. Не всегда программы, созданные под распространенные операционные системы, например, под Windows, совместимы с платформой Linux.

Обратим внимание на некоторые разработки.

ALT Linux. Разработка ведётся с 1998 года, но производители предпочитают считать её с начала проекта Sisyphus в 2000 году. За последние 6 лет отправлено в эксплуатацию около 150 тысяч несертифицированных и 50 тысяч сертифицированных ФСТЭК продуктов. Основной продукт Альт является проект Sisyphus. Идёт работа над репозиторием системы «Эльбрус». Генеральный директор Базальт СПО заявляет, что инфраструктура, пакеты и дистрибутивы не копируются, а пишутся участниками проекта.

Astra Linux. Как утверждают разработчики Astra Linux, операционная система версии Special Edition: «надёжна и безопасна настолько, насколько безопасным может быть самый защищённый от злоумышленников дверной замок: врежьте его в деревянную дверь, и вот от него уже нет никакого смысла». Операционная система сегодня реализует все самые актуальные способы защиты информации от несанкционированного доступа, за исключением криптографических, а организация архитектуры реализующих эти способы средств, непрерывная работа над обновлениями и правильная ее эксплуатация пользователями и администраторами являются существенным фактором снижения рисков потери конфиденциальности, целостности и доступности информации.

Sailfish Mobile. Это не «еще один Linux» несмотря на то, что архитектурно – это действительно знакомый всем Linux. Эта система работает на любых мобильных устройствах любых производителей, что, как мы видим, является достаточно сложной технологической задачей, и то, что разработчики её решили – это, безусловно, уникальная особенность Sailfish Mobile OS RUS. Принципиальное отличие Sailfish Mobile OS RUS – возможность для заказчиков построить защищенное мобильное решение, которое будет находиться полностью внутри периметра организации. Это позволяет создавать корпоративные мобильные решения фактически любого уровня доверия за существенно меньшие деньги.

Таким образом, обратив внимание на некоторые моменты, необходимо разработать определённую систему требований, применяемых к операционным системам специального назначения, по направлениям функциональной полноты и эксплуатационных требований (расширяемость, переносимость, совместимость, надёжность, безопасность, производительность).

В результате должны быть разработаны требования и предложения по эксплуатации операционных систем специального назначения с учётом особенностей и условий их эксплуатации и применения.

Выполнение разработанных требований позволит упростить и сделать наиболее эффективным выбор операционных систем для решения конкретных задач.

Переход муниципалитетов с Windows на операционные системы, разработанные российскими компаниями, это шаг, который «увеличит технологическую независимость нашей страны» и повысит эффективность обеспечения безопасности государства.

СПИСОК ЛИТЕРАТУРЫ

1. Безопасность операционной системы специального назначения ASTRA LINUX SPECIAL EDITION. УЧЕБНОЕ ПОСОБИЕ Для ВУЗОВ / Под редакцией доктора техн. наук П.Н. Девянина. Буренин П.В., Лебеденко Е.В., Проскурин В.Г., Цибуля А.Н. 2-е издание, 2016 г. 312 стр.
2. Книга: Э.С. Спиридонов, М.С. Клыков, М.Д. Рукин, Н.П. Григорьев, Т.И. Балалаева, А.В. Смуров «Операционные системы. Учебник» Издательство: "Либроком", 2015 г., 350 стр.

УДК 004.942.001.57

ПРОГРАММА ДЛЯ МОДЕЛИРОВАНИЯ ОБЪЕКТОВ – SKETCHUP

Шибанов Данил Сергеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: shibanovd94@mail.ru

Аннотация. Задача 3D моделирования - разработать визуальный объёмный образ желаемого объекта. С помощью трёхмерной графики можно создать точную копию существующего объекта, а также разработать новую модель. Трехмерная графика активно применяется для создания изображений на плоскости экрана или листа печатной продукции в науке и промышленности, например, в системах автоматизации проектных работ, архитектурной визуализации.

Ключевые слова: *3D моделирование; модель; окно программы; объект; визуализация.*

PROGRAM FOR MODELING OBJECTS – SKETCHUP

Shibanov Danil
S.M. Budjonny Military Academy of the Signal Corps
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail: shibanovd94@mail.ru

Abstract. The task of 3D modeling is to develop a visual 3D image of the desired object. Using 3D graphics, you can create an exact copy of an existing object, as well as develop a new model. Three-dimensional graphics are actively used to create images on the screen plane or sheet of printed matter in science and industry, for example, in automation systems for design work, architectural visualization.

Keywords: *3D modeling; model; program window; object; visualization.*

Развитие последних технологий ясно демонстрирует совершенствование методов сбора трехмерных данных о местности и объектах в отношении повышения точности и разрешения. В научных исследованиях широко применяется компьютерное картографирование, характеризующееся высокой степенью автоматизации, интерактивностью, применением мультимедиа и компьютерного дизайна, созданием новых видов изображений и т.д.

SketchUp – программа для создания трехмерных моделей домов, мебели, интерьера, различных архитектурных строений. В марте 2006 года была приобретена компанией Google вместе с небольшой фирмой Last Software. В апреле 2012 Google продал SketchUp компании Trimble Navigatio. Существуют две версии программы – бесплатная для не коммерческого использования, ограниченная по функциональности SketchUp Make и платная SketchUp Pro [1].

Основным преимуществом SketchUp, является способность программы подсказывать наиболее удобный следующий ход и способ действия – в любой момент построений она выводит на экран графические и текстовые подсказки (левый нижний угол), опираясь на которые можно легко и быстро работать [2].

В данной программе полностью отсутствуют окна предварительных настроек и присутствует такая функция как push/pull (тяни/толкай), это и есть главные ее отличительные особенности от других программ.

Функции SketchUp [3]:

– Push/pull (тяни/толкай) – это быстрый переход от 2D модели к 3D. Является запатентованным инструментом.

– Заливка, с помощью которой можно задавать текстуры и различные цвета моделям.

– Точные измерения. В программе используется электронный карандаш, который позволяет делать точные измерения модели.

– Тени и сечения.

– Сцены и анимации.

– Учебник. В диалоговом окне есть раздел учебник, который предоставляет пользователю необходимую информацию для каждого случая.

– Архив моделей.

– Работа с рельефом. Инструменты Песочницы в SketchUp позволяют создавать, адаптировать и изменять изображение местности в 3D. С помощью набора импортированных контурных линий можно создать гладкий ландшафт, добавить уступы и долины и автотрассы.

– Google Планета Земля. Просмотр моделей с учетом местных условий. SketchUp и Google Планета Земля входят в одну и ту же группу продуктов, т. е. обмен данными между этими программами проходит легко и просто. Если необходимо получить изображение места создания проекта можно одним нажатием кнопки импортировать масштабированный аэрофотоснимок с топографией из Google Планета Земля в SketchUp.

Обычно 3D-проекты нуждаются в чертежах и схематичных рисунках. В SketchUp Pro есть возможность создавать из проектов макеты с рисунками, в которых можно редактировать текстуры, регулировать толщину линий, а также дополнять чертежи размерами, выносками и другой графикой. Изменения автоматически отражаются в макете. SketchUp Pro позволит экспортировать модели и макеты в изображения, PDF-файлы [4].

На данный момент самой новой версией программы является SketchUp – 2015 версия как для профессионалов, так и для новичков. Создавая свои модели, пользователи могут размещать их в онлайн коллекциях Google.

Очевидно, что программное обеспечение SketcUp используется в основном из-за простого интерфейса моделирования, доступного даже начинающему пользователю, бесплатности программы, а также следует отметить небольшой размер дистрибутива, большой каталог бесплатно доступных 3D моделей, и наличие большого количества бесплатных расширений на языке Ruby. Из недостатков можно отметить не кроссплатформенный, нет версии под Linux.

СПИСОК ЛИТЕРАТУРЫ

1. Интернет ресурс: Свободная энциклопедия. https://ru.wikipedia.org/wiki/SketchUp
2. Интернет ресурс: Журнал Научно-технический интернет. http://www.architector.dp.ua/ sketchup/5/4/Sketchup---nemnogo-o-programme.htm
3. Интернет ресурс: Компьютерный журнал. http://www.ixbt.com/news/soft/index.shtml?17/73/45/
4. Интернет ресурс: Программное обеспечение для компьютеров. http://www.softsalad.ru/software/sketchup.html

УДК 681.5.391.21

АКТУАЛЬНОСТЬ РАЗВИТИЯ СЕТЕВОГО КОНТРОЛЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Шостак Роман Константинович[1], Лепешкин Олег Михайлович[2]
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: kryptograf@yandex.ru

Аннотация. В докладе рассмотрены вопросы функционирования существующей системы контроля и мониторинга защищенности инфокоммуникационных сетей в современных условиях, и актуальность развития сетевого контроля систем связи в целях обеспечения своевременности обнаружения деструктивных воздействий на сеть.

Ключевые слова: *киберпространство; информационная сфера; информационное оружие; информационный терроризм; электронные скорости.*

THE RELEVANCE OF THE DEVELOPMENT OF NETWORK MONITORING SECURITY INFORMATION SYSTEMS

Shostak Roman[1], Lepeshkin Oleg[2]
[1] St. Petersburg State Military academy of communications named after Marshal of the Soviet Union S.M. Budenny
[2]Dr. of Tech. Sci., senior teaching Department “Security of infocommunication systems of a special purpose”
St. Petersburg, Russia, Tihoretckij pr., 3
e-mail: kryptograf@yandex.ru

Abstract. The report tells about questions of functioning of existing control and monitoring system of infocommunication networks in actual conditions and relevance of developing of system communication network monitoring for timeliness of detection of blasting software impact on the network.

Keywords: *cyberspace,information field, informational weapon, information terrorism, electronic speed.*

Сетевой контроль информационно-телекоммуникационных систем, систем связи специального назначения позволит осуществлять мониторинг их комплексного состояния, обеспечить достаточную своевременность обнаружения деструктивных воздействий на систему в киберпространстве, и, как следствие, своевременное принятие эффективных мер противодействия, что значительно повысит

эффективность мероприятий безопасности, а равно и защищенность инфокоммуникационных систем любого уровня.

Материальной основой информационной сферы является единое информационно-телекоммуникационное пространство страны, как база решения задач социально-экономического, политического, военного, научного и культурного развития страны и обеспечения ее безопасности.

Современные сети и коммуникации должны оперативно реагировать на атаки, сохраняя свою доступность, надежность и работоспособность. Во многих отношениях целью процесса обеспечения безопасности является повышение отказоустойчивости сетей. Вместо того, чтобы становиться «жертвами», сети должны быть способными «поглощать» атаки и сохранять работоспособность. Специалисты в области безопасности различают три основных слоя киберпространства: физический (инфраструктура, кабели, маршрутизаторы и коммутаторы), семантический (передаваемые в киберпространстве необработанные данные, которые использует машина или человек) и синтаксический (связывает между собой два предыдущих путем форматирования информации в соответствии со стандартами и протоколами, как, например, TCP/IP, на котором и держится весь интернет)[1].

Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, применяемые информационные технологии и особенности (условия) функционирования информационной системы [2].

Любое программное или аппаратное обеспечение не является совершенным, и всегда можно предположить, что в нем найдутся уязвимости, позволяющие совершить какие-либо действия, нарушающие установленный порядок использования ресурсов. Кроме того, реагирование на несанкционированную активность или попытки взлома системы в режиме близком к реальному времени практически невозможно, если эти функции выполняются вручную.

Сетевой контроль информационно-телекоммуникационных систем должен позволять осуществлять мониторинг их комплексного состояния, обеспечить достаточную своевременность обнаружения деструктивных воздействий на систему в киберпространстве, и, как следствие, своевременное принятие эффективных мер противодействия.

Интернет давно стал неотъемлемой частью не только повседневной жизни граждан, но и таких серьезных систем как биржи или системы управления, вплоть до городского транспорта или банка. Атака на подобные системы, правительственные серверы, может повлечь за собой вполне серьезные последствия или социальные потрясения, внести разлад в повседневную жизнь страны, нарушить управление военной или гражданской инфраструктурой[3].

Существующая система сертификации оборудования и проверки на предмет наличия «закладок» не позволяет в полной мере быть уверенным в том, что «закладки» в закупаемом за рубежом оборудовании выявлены в полном объеме. Оборудование, закупаемое для ЕСЭ РФ, вообще не подвергается такого рода проверкам и сертификации.

Следует отметить, что межузловые связи создаются, как правило, с использованием каналов, арендованных у операторов связи.

При этом, магистральные сети операторов связи, предоставляющих сетям связи специального назначения ресурсы ЕСЭ РФ, разветвленной сетью выходят далеко за пределы РФ.

Естественным в таких условиях является рост количества угроз информационной безопасности. При этом, в качестве своего рода информационного оружия, для эффективного воздействия на противника все большее значение приобретает техническая компьютерная разведка для выявления элементов скрытого управления, состава системы, ее структуры, элементов системы защиты и т.д. Информационное оружие может использоваться с «электронными скоростями» при нападении и обороне. Оно базируется на самых передовых технологиях и призвано обеспечить разрешение военных конфликтов на ранней стадии, а также исключить применение сил общего назначения. Стратегия применения информационного оружия носит наступательный характер. Однако есть понимание собственной уязвимости, особенно гражданского сектора, поэтому проблемы защиты от такого оружия и информационного терроризма сегодня вышли на первый план.

В современном обществе военная стратегия использования информационного оружия оказалась тесно связанной с гражданским сектором и стала во много от него зависеть. Разнообразие информационного оружия, форм и способов его воздействия, особенности появления и применения породили сложнейшие задачи защиты от него.

Несмотря на то, что средства обнаружения атак продолжают развиваться, бороться с угрозами со стороны неконтролируемо растущей сети Интернет становится все труднее[4].

Заключение. Во многих отношениях целью процесса обеспечения безопасности является повышение отказоустойчивости сетей, сети должны быть способными «поглощать» атаки и сохранять

работоспособность. Обеспечить эти требуемые свойства безопасности и надежности информационных систем, в особенности сетей связи специального назначения, и призвано дальнейшее развитие сетевого контроля информационных систем и сетей связи специального назначения.

СПИСОК ЛИТЕРАТУРЫ

1. Лепешкин О.М., Корсунский А.С. Оптимизация структуры комплекса информационно-технических средств в автоматизированных системах управления. Автоматизация процессов управления. № 4. 2011, 76-81 с.
2. Карпов А.В., Лепешкин О.М., Попов Н.А. Структура электромагнитного поля при нелинейной радиолокации. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С.1118.
3. Лепешкин О.М., Карпов А.В., Шостак Р.К.Актуальность осуществления сетевого контроля защищенности информационных сетей. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1198.
4. Стародубцев Ю.И., Бречко А.А., Львова Н.В. Необходимость оценки защищенности системы связи от средств информационной борьбы в современных условиях. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1201.

УДК 681.5.391.21

ИНТЕГРИРОВАННЫЙ МОНИТОРИНГ ПОДВИЖНЫХ ОБЪЕКТОВ СВЯЗИ

Шостак Роман Константинович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail: kryptograf@yandex.ru

Аннотация. В докладе рассмотрены вопросы подхода к мониторингу подвижных объектов связи, систем управления и связи в целях обеспечения их доступности, надежности и работоспособности.

Ключевые слова: *надежность; работоспособность; подвижные объекты связи.*

THE APPROACH OF INTEGRATED MONITORING OF MOBILE OBJECTS OF COMMUNICATION

Shostak Roman
St. Petersburg State Military academy of communications
named after Marshal of the Soviet Union S. M. Budenny
St. Petersburg, Russia, Tihoretckij pr., 3
e-mail: kryptograf@yandex.ru

Abstract. The report discussed the approach of monitoring of mobile communication facilities, systems of control and communication in order to ensure their availability, reliability and efficiency.

Keywords: *reliability; efficiency; mobile communication.*

Разнообразие информационного оружия, форм и способов его воздействия, особенности появления и применения породили сложнейшие задачи защиты от него.

Целью процесса обеспечения безопасности сетей связи является повышение их отказоустойчивости, сети должны быть способными «поглощать» атаки и сохранять работоспособность. Обеспечить эти требуемые свойства безопасности и надежности информационных систем, в особенности сетей связи специального назначения, и есть наиважнейшая задача[1].Сетевой контроль информационно-телекоммуникационных систем, систем связи специального назначения позволит осуществлять мониторинг их комплексного состояния, обеспечить достаточную своевременность обнаружения деструктивных воздействий на систему в киберпространстве, и, как следствие, своевременное принятие эффективных мер противодействия, что значительно повысит эффективность мероприятий безопасности [2].

Любое программное или аппаратное обеспечение не является совершенным, и всегда можно предположить, что в нем найдутся уязвимости, позволяющие совершить какие-либо действия, нарушающие установленный порядок использования ресурсов.

Анализируя полевую составляющую системы управления и сети связи силовых структур, следует сделать вывод, что совершенствование организации и способа их развертывания на местности позволило повысить их разведзащищенность и живучесть в условиях интенсивного развития высокоточного оружия и средств разведки.

Эффективность принимаемых мер защиты зависит от качества определения угроз для конкретной информационной системы в конкретных условиях ее функционирования.

Современные сети и коммуникации должны оперативно реагировать на атаки, сохраняя свою доступность, надежность и работоспособность. Во многих отношениях целью процесса обеспечения безопасности является повышение отказоустойчивости сетей [3].

При существующих принципах построения систем управления и сетей связи подвижного сегмента для их функционального взаимодействия в едином информационном пространстве и выполнения задач по обеспечению устойчивого информационного обмена, необходим новый подход к мониторингу подвижных объектов связи, который обеспечивал бы выполнение следующих функций:

– предварительно задавать вид и уровень опасности неисправностей подсистем и систем вцелом, соответствующие им пороговые значения параметров технического состояния, допустимые значения функциональных параметров, разрешенные режимы функционирования и допустимые значения параметров регламентного состояния сетей связи;

– диагностировать параметры технического состояния контролируемого объекта при помощи расположенных на них компьютерных средств мониторинга и диагностики регламентного состояния;

– формировать управляющее воздействие по ближайшим неотложным действиям, направленным на устранение неисправностей и нарушений в режимах работы, недопущение развития уровня опасности и снижение влияния неисправностей и нарушений на безопасность объекта и системы в целом;

– формировать сводную диагностическую информацию о регламентном состоянии контролируемой системы;

– автоматически формировать сводную информацию о нарушениях установленных режимов функционирования;

– отображать результаты контроля на экране средства мониторинга;

– сравнивать измеренные значения параметров регламентного состояния с предварительно заданными значениями;

– оценивать техническое состояние узлов, агрегатов, подсистем и объекта в целом;

– фиксировать нарушения предварительно заданных разрешенных режимов функционирования;

– автоматически определять вид и уровень опасности неисправностей и нарушений установленных регламентных состояний;

– автоматически формировать управляющий сигнал (воздействие) по ближайшим неотложным действиям, направленным на определение неисправного элемента, узла, агрегата, недопущение развития уровня опасности неисправности и снижения влияния неисправности на безопасность объекта.

Совершенствование подходов к мониторингу состояния подвижных объектов связи позволит обеспечить непрерывное поддержание доступности, надежности и работоспособности подвижных объектов связи, систем управления и сетей связи в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Лепешкин О.М., Карпов А.В., Шостак Р.К.Актуальность осуществления сетевого контроля защищенности информационных сетей. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 1198.
2. Лепешкин О.М., Корсунский А.С. Оптимизация структуры комплекса информационно-технических средств в автоматизированных системах управления. Автоматизация процессов управления. № 4. 2011, 76-81 с.
3. Карпов А.В., Лепешкин О.М., Попов Н.А. Структура электромагнитного поля при нелинейной радиолокации. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С.1118.

УДК 004.056.53

ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИИ В СЕТЯХ С ВЫСОКИМ УРОВНЕМ КОНФИДЕНЦИАЛЬНОСТИ

Штаненко Василий Иванович, Барауля Игорь Геннадьевич, Маслов Олег Николаевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр., 3
e-mail:shteff81@mail.ru

Аннотация. В докладе рассмотрен подход к защите информации в сетях с высоким уровнем конфиденциальности – создание замкнутой компьютерной системы (ЗКС) с применением «классических» программно-аппаратных средств, обеспечивающих высокую степень защиты информации на автоматизированных рабочих местах (АРМ) сетей с высоким классом защиты.

Ключевые слова: *автоматизированное рабочее место; модуль доверенной загрузки; несанкционированный доступ; средства разграничения доступа.*

THE DESIGN METHOD OF SYSTEM ACCESS SECURITY

Shtanenko Vasily, Baraulya Igor, Maslov Oleg
Military Academy of communications
Russia, St. Petersburg, Tikhoretsky pr., 3
e-mail:shteff81@mail.ru

Abstract. In the report approach to information security on networks with the high level of confidentiality – creation of the closed computer system (CCS) using the "classical" software and hardware

tools providing high degree of protection of information on the automated jobs (AJ) of networks with a high class of protection is considered.

Keywords: *workstation; trusted boot module; unauthorized access; access control system.*

Проблемы защиты информации от несанкционированного доступа при ее обработке и хранении на автоматизированных рабочих местах являются весьма актуальными в мире современных информационных технологий [1].

По сообщению аналитического центра Zecurion Analytics [2] по числу утечек (49 публичных инцидентов) Россия стоит на 4-м месте после США (абсолютный лидер, 72% от всех зарегистрированных 868 инцидентов в мире), Великобритании и Канады.

Статистика наличия умысла в несанкционированных действиях показывает тенденцию к увеличению целенаправленных атак (более 32 %), в том числе с участием сотрудников внутри организаций (учреждений, компаний), при этом случайные утечки за счет халатности сотрудников составили около 37%. Больше всего конфиденциальной информации (22%) утекает через интернет (веб-сервисы).

Одним из основных способов обеспечения защиты от несанкционированного доступа (НСД) к информации, обрабатываемой в информационно-вычислительных системах, является создание замкнутой компьютерной системы (ЗКС). Особенно это важно при использовании зарубежных вычислительных средств.

Для создания замкнутой среды разработан широкий ассортимент устройств, призванных ограничить потенциально злонамеренные возможности недоверенного компьютера [3]. Они обеспечивают строго регламентированный доступ к автоматизированным рабочим местам (АРМ) и регламентируют или полностью ограничивают доступ к транспортной среде.

Средства создания замкнутой среды можно разделить на две категории:

защита от прямого доступа злоумышленника или недобросовестного сотрудника к АРМ: включение, загрузка операционной системы (ОС), вход в систему и получение доступа к ресурсам;

защита каналов связи локальной вычислительной сети (ЛВС), т.е. защита АРМ от НСД по сети.

Создание замкнутой среды для АРМ с одним пользователем можно построить с помощью аппаратно-программных модулей доверенной загрузки (АПМДЗ), доверенных систем запуска компьютера (BIOS), средств виртуализации и средств защиты от атак из ЛВС. Для многопользовательского АРМ для создания ЗКС для каждого пользователя дополнительно применяется система (или средство) разграничения доступа (СРД) [4]. С целью предотвращения доступа к информации на жестком диске в случае разукомплектования АРМ или его кражи применяются шифраторы диска, обеспечивающие криптографическую защиту хранящейся на нем информации.

Применение «классических» программно-аппаратных средств обеспечит высокую степень защиты информации на АРМ.

Наиболее полно функции аппаратно-программного модуля доверенной загрузки [5] реализованы в АПМДЗ ведущих разработчиков: линейки изделий «КРИПТОН-ЗАМОК» ООО «Фирма АНКАД», средств защиты информации от НСД серии «Аккорд», АПМДЗ «Соболь» ООО «Код безопасности».

Использование системы разграничения доступа предоставит каждому пользователю доступ только к определенным программным и аппаратным ресурсам, а также к информации определенного уровня. Также позволит осуществить динамический и статический контроль за каждым пользователем по доступу к ресурсам АРМ [6].

Как правило, система разграничения доступа привязана к АПМДЗ. Большинство систем защиты от НСД в той или иной степени реализуют возможности СРД. Наиболее полно функции АПМДЗ и СРД реализованы в семействе изделий "КРИПТОН-ЗАМОК" (СРД "КРИПТОН-ЩИТ"), средствах защиты серии «Аккорд» и продукте "Secret Net" (ООО "Код безопасности").

Данный подход позволит обеспечить защиту информации в сетях с высоким уровнем конфиденциальности и предотвратить несанкционированный доступ на эти объекты.

СПИСОК ЛИТЕРАТУРЫ

6. Лепешкин О.М. ИССЛЕДОВАНИЕ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ. Инфокоммуникационные технологии. 2007. Т. 5. № 3. С. 165-166.
7. Утечки конфиденциальной информации в России и мире. Итоги 2016 года. Аналитический обзор Zecurion Analytics, www.zecurion.ru
8. Рябко С.Д. Угрозы недоверенного рабочего места пользователя и методы защиты от них. Информационная безопасность. TComm. Спецвыпуск. 2012 С.26-30.
9. Хорев П.Б. Анализ средств разграничения доступа к объектам в операционных системах Microsoft Windows Linux // Электронный журнал "Вычислительные сети. Теория и практика" 2009. №2 (15).
10. Лепешкин О.М., Харечкин П.В. Анализ моделей разграничения доступа, реализованных в современных социотехнических системах. Инфокоммуникационные технологии. 2008. Т. 6. № 2. С. 91-93.
11. Краснокутский А.В., Лепешкин О.М., Харечкин П.В. Анализ функциональной применимости ролевой модели разграничения доступа в системах управления. Инфокоммуникационные технологии. 2007. Т. 5. № 3. С. 162-164.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

УДК 004.056.53

ИССЛЕДОВАНИЕ СОЗДАНИЯ БЕЗОПАСНЫХ ПРОГРАММ ДЛЯ ВЫСОКОПРОИЗВОДИТЕЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ ПЛАТФОРМЫ

Бежан Роман Романович, Медведев Михаил Сергеевич, Арустамов Сергей Аркадьевич
Университет ИТМО,
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: romanbezhan@gmail.com,mmedvedev.793@mail.ru, sergey.arustamov@gmail.com

Аннотация. Рассмотрены способы создания безопасных программ на примере высокопроизводительной вычислительной платформы SAPHANA, различные реализации и сценарии атак, а также методы их защиты. В ходе исследования был использован подход - исследование безопасных программ с применением готовых автоматических программных решений.

Ключевые слова*: JavaScript; XSJS; высокопроизводительная вычислительная платформа; SAP HANA; UI, безопасность программ.*

RESEARCH OF CREATION OF SAFE PROGRAMS FOR THE HIGH-PERFORMANCE COMPUTING PLATFORM

Bezhan Roman, Medvedev Mikhail, Sergey Arustamov
St. PetersburgNational Research University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverksky pr.,49
e-mails: romanbezhan@gmail.com, mmedvedev.793@mail.ru, sergey.arustamov@gmail.com

Abstract. The article presents different ways of creation of secure programs by example of ERP SAP HANA, various attack scenarios and implementation, as well as ways of securing programs. In the time of research there was special kind of analysis used – the analysis with the implementation of ready-made automatic software-based solutions.

Keywords: *JavaScript; XSJS; Enterprise Resource Planning; SAP HANA; UI5; application security.*

В быстро меняющимся информационном мире ежедневно создаются новые информационные технологии, которые успешно находят свое применение в бизнесе. Но с использованием новых технологий, неизбежно появляются новые риски их использования благодаря невыявленным возможным программным уязвимостям. Лидером по созданию высокопроизводительных вычислительных платформ является компания SAP, головной офис которой расположен в Германии. В качестве высокопроизводительной вычислительной платформы, для исследования создания безопасных программ, была выбрана система SAP HANA с установленным фреймворком UI5. SAP HANA – это специализированная бизнес платформа, основной особенностью которой, является использование оперативной памяти для вычислений аналитики в режиме реального времени (технология «In Memory»), а также создание и использование программ для управления бизнес процессами [1].

Для исследования создания безопасных программ для высокопроизводительной вычислительной платформы SAP HANA, за список возможных угроз была выбрана выборка часто встречаемых угроз в программах согласно исследованию, за 2017 год открытого проекта по безопасности OWASP [2]. Были рассмотрены угрозы: уязвимость внедрения кода, некорректная аутентификация и управление сессией, межсайтовый скриптинг, ослабленный контроль доступа, небезопасная конфигурация, утечка чувствительных данных, недостаточная защита от атак, подделка межсайтовых запросов, использование компонентов с известными уязвимостями, недостаточно защищенные API. Угрозы были изучены и применены согласно контексту высокопроизводительной вычислительной платформы.

В процессе исследования был сконфигурирован специализированный стенд, для разработки безопасных программ для высокопроизводительной вычислительной платформы, на примере открытого решение Eclipse Luna [3]. В качестве первоначально тестируемых приложений были выбраны программы, основой которых служит язык XSJS. XSJS - язык программирования, созданный компанией SAP на основе языка JavaScript. Были написаны программы на данном языке с учетом выборки часто встречаемых угроз проекта OWASP. При исследовании созданных приложений

использовалось готовое программное решение – сканер уязвимостей и исходного кода CheckMarx. Данный сканер выявил устаревшую версию библиотеки пакета jQuery [4], которая имела в себе уязвимость межсайтового скриптинга DOM. Дальнейшее исследование показало, что уязвимость была закрыта специальным дополнительным кодом, написанным отдельно от данной библиотеки.

Заключение. В ходе создания безопасных программ для высокопроизводительной вычислительной платформы на примере платформы SAP HANA и программ на языке XSJS были выявлены угроза, согласно выборке открытого проекта по обеспечению OWASP, а также ее закрытие средствами производителя. Так как исследование проводилось с применением готовых автоматических программных решений, в дальнейших планах проведение анализа вручную. Также, учитывая другие поддерживаемые языки программирования для написания собственных бизнес приложений платформой SAP HANA, предполагается рассмотреть другие языки, помимо XSJS.

СПИСОК ЛИТЕРАТУРЫ

1. Хабрахабр, блог компании SAP [Электронный ресурс] / Режим доступа: http://habrahabr.ru/company/sap/blog/252539/ (18.09.2017)
2. OWASP, Top 10 Application Security Risks [Электронныйресурс] / Режимдоступа: https://www.owasp.org/index.php/Top_10_2017-A2-Broken_Authentication_and_Session_Management (18.09.2017)
3. Википедия, Eclipse [Электронный ресурс] / Режим доступа: https://ru.wikipedia.org/wiki/Eclipse_(среда_разработки) (18.09.2017)
4. Википедия, jQuery [Электронный ресурс] / Режим доступа: https://ru.wikipedia.org/wiki/JQuery (18.09.2017)

УДК 614.2

УСЛОВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЛИНИЧЕСКОЙ СФЕРЕ СИСТЕМЫ ЗДРАВООХРАНЕНИЯ

Блюм Владислав Станиславович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14 линия, 39
e-mail: vlad@blum.spb.su

Аннотация. В статье рассмотрены условия информационной безопасности пациентов, которая обеспечивается новой организацией цифровой клинической медицинской информации и достижением ею свойств полноты, достоверности и доступности для автоматизированной обработки. Рассмотрена телекоммуникационная структура единой государственной информационной системы здравоохранения, обеспечивающей сбор и сохранение полного объёма первичной медицинской информации. Предложена динамическая информационная (математическая) модель полной, достоверной и доступной для автоматизированной обработки первичной медицинской информации. Модель описывает процесс сбора электронных персональных медицинских записей и формирования федеральной базы интегрированных электронных медицинских карт.

Ключевые слова: *информационная безопасность пациентов; электронная персональная медицинская запись; интегрированная электронная медицинская карта.*

CONDITIONS OF INFORMATION SECURITY IN THE CLINICAL SPHERE OF THE HEALTH SYSTEM

Blum Vladislav
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39
e-mail: vlad@blum.spb.su

Abstract. The article considers the information security conditions for patients, which is provided by a new organization of digital clinical medical information and the achievement of its completeness, reliability and accessibility features for automated processing. The telecommunication structure of the unified state health information system providing collection and preservation of the full volume of primary medical information is considered. A dynamic information (mathematical) model of complete, reliable and accessible for automated processing of primary medical information is proposed. The model describes the process of collecting electronic personal medical records and the formation of a federal database of integrated electronic medical records.

Keywords: *information safety of patients; electronic personal medical record; integrated electronic medical record.*

Введение.

Раннее обнаружение дефектов оказания медицинской помощи всегда было и остаётся одной из наиболее актуальных и острых проблем в сфере здравоохранения. Согласно данным, опубликованным в British Medical Journal (2016 г), в рейтинге причин смертности, дефекты оказания медицинской помощи заняли уверенное третье место, после сердечно-сосудистых и онкологических заболеваний. Ежегодно от этих причин погибает около 250 тысяч американцев.

Пути повышения информационной безопасности пациентов следует искать в интенсивной цифровизации информационной составляющей клиничекой сферы здравоохранения.

Ожидания качественных изменений в способах решения проблемы раннего обнаружения дефектов оказания медицинской помощи связывают с переходом на электронный документооборот (цифровизацию) в клинической сфере здравоохранения. Использование компьютера для формирования персональных медицинских записей (ПМЗ) врачами и диагностическими лабораториями, а также интегрирование ПМЗ в электронные медицинские карты в региональных и федеральном центрах обработки данных (ЦОД) создают условия для превращения системы здравоохранения в социальную иммунную систему, которая не только непрерывно контролирует состояние каждого гражданина страны, но и способна оперативно концентрировать необходимые ресурсы для борьбы с вторжениями болезней.

Основой (ядром) системы охраны здоровья России является её клиническая компонента, то есть та часть системы, в которой реализуются лечебно-диагностические процессы (ЛДП). Исполнительными органами, эффекторами ЛДП являются дипломированные медицинские сотрудники и лицензированные медицинские диагностические лаборатории. Именно эти участники ЛДП образуют два класса квалифицированных источников медицинской информации (КИМИ), которые формируют поток первичной медицинской информации в клинической сфере здравоохранения.

Ещё недавно сбор и оперативная обработка подобного потока сложной информации, источники которой распределены по всей стране, были технологически не реализуемы. Напомним, что годовой объём первичной медицинской информации составляет 3-5 терабайта [1], с интенсивностью более миллиона персональных медицинских записей в сутки, при большом структурном разнообразии и высокой семантической сложности.

Тем не менее, для решения проблемы раннего обнаружения дефектов оказания медицинской помощи и повышения эффективности лечебно-диагностических процессов необходимо обеспечить интегрирование первичной медицинской информации, гарантировать её полноту, достоверность и доступность для автоматизированной обработки.

В настоящее время проблема сбора и обработки «больших данных» – полного потока клинической информации перешла в технологическую плоскость.

1. Федеральный сервис «Интегрированная электронная медицинская карта».

В состав Единой государственной информационной системы в сфере здравоохранения Российской Федерации входит федеральный сервис интегрированной электронной медицинской карты [http://zakupki.gov.ru], который должен быть реализован с использованием сервисно-ориентированных и облачных технологий. Решение проблемы цифрового представления полного, достоверного и доступного для автоматизированной обработки массива первичной медицинской информации лежит в основе цифровизации здравоохранения. Как указано в техническом задании, «основной целью ведения Интегрированной электронной медицинской карты (далее ИЭМК) является обеспечения непрерывности, преемственности и качества лечения, а также своевременной профилактики и иных мероприятий по обеспечению здоровья конкретного индивида путем документирования и сохранения соответствующей медицинской информации и своевременного предоставления ее уполномоченным медицинским работникам и организациям, а также субъектам ИЭМК.»

Под ИЭМК следует понимать коллекцию ЭПМЗ, которая включает все, без исключения, упорядоченные по времени медицинские записи, которые сделали КИМИ по поводу конкретного пациента, независимо от того, в каком ЛПУ или медицинской диагностической лаборатории страны эта запись выполнена.

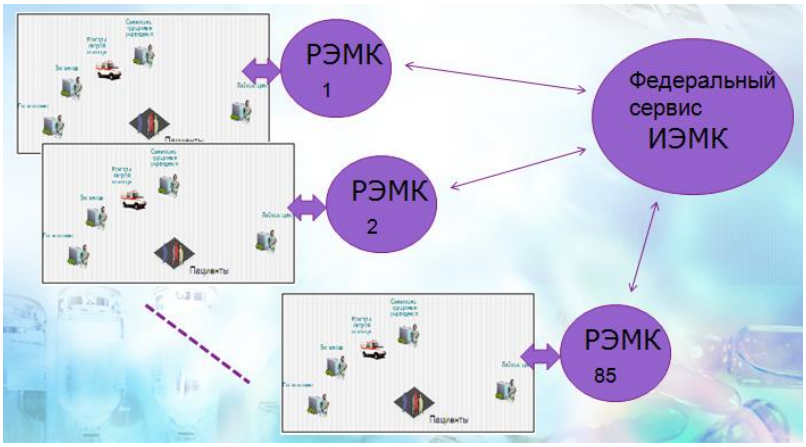


Рисунок 1. Инфраструктура клинической сферы системы здравоохранения России

На рис.1 приведена схема трёхуровневой медицинской информационной системы клинической сферы здравоохранения России. Согласно этой схеме поток первичной медицинской информации (поток ЭПМЗ), формируемых КИМИ, имеет три уровня интеграции: в базе ЭМК лечебно-профилактического учреждения (ЛПУ), в базах ИЭМК региональных центров обработки информации (ЦОД), а затем в базе ИЭМК федерального ЦОД. Такой подход гарантирует полноту и достоверность клинической информации для её дальнейшего использования в лечебно-диагностическом процессе.

Электронная история болезни и персональная электронная медицинская запись.

Электронная история болезни (ЭИБ) согласно ГОСТ [ГОСТ Р 52636-2006] – это «информационная система, предназначенная для ведения, хранения на электронных носителях, поиска и выдачи по информационным запросам (в том числе и по электронным каналам связи) персональных медицинских записей.» ЭИБ состоит из размещённых в хронологической последовательности электронных персональных медицинских записей (ЭПМЗ). Понятие "электронная персональная медицинская запись" соответствует международному термину EHR – Electronic Health Record [1].

Определяющими свойствами ЭПМЗ являются:

– во-первых, ЭПМЗ создают квалифицированные источники медицинской информации,

– во-вторых, ЭПМЗ – это неделимая и неизменяемая запись истории болезни (электронной истории болезни).

Синтаксическая структура ЭПМЗ на метаязыке может быть представлена в виде:

<ЭПМЗ > :: = <время сеанса>< идентификатор КИМИ>
< идентификатор ПАЦИЕНТА>< документ КИМИ> (1)

< идентификатор КИМИ> :: = < идентификатор МР > | < идентификатор ДЛ>, где
< идентификатор МР > – идентификатор медицинского работника,
<идентификатор ДЛ>– идентификатор медицинской диагностической лаборатории.

Обратим внимание на два обязательных атрибута ЭПМЗ, на <время сеанса> и <идентификатор ПАЦИЕНТА>.

Обозначим ЭПМЗ, сделанную j -м врачом по поводу i-го пациента, как $z(i, j, t)$, где t– время, указанное в ЭПМЗ, а соответствующее событие обозначим как – $\breve{z}(i, j, t)$. Выделим два особых вида ЭПМЗ и соответствующих событий: записи, в которых врач фиксирует появление (рождение) нового пациента, обозначим – $z_0(i, j, t)$, а записи, в которых врач констатирует смерть пациента, обозначим – $z_f(i, j, t)$. Эти события обозначим как $\breve{z}_0(i, j, t)$, $\breve{z}_f(i, j, t)$.

В случае, когда все ЭПМЗ поступают в ЦОД, можно говорить о том, что интегрированная электронная медицинская карта (ИЭМК) есть функция распределения информации о здоровье пациента. Эта информация добыта системой здравоохранения на всём интервале жизни пациента. Действительно, каждая ЭПМЗ имеет обязательный параметр – время её создания. В результате формирования ИЭМК фиксируется ряд интервалов времени от рождения до смерти пациента, задающих частоту взаимодействий пациента с системой здравоохранения. Кроме того, каждая встреча пациента с КИМИ связана с приращением информации о состоянии здоровья пациента, которая накапливается в ИЭМК. Очевидно, что количество таких приращений соответствует числу временных интервалов. Соответствие временных и информационных интервалов нарушается, только в момент смерти пациента. После этого события информационное приращение (заключение врача о смерти) имеет место, а соответствующий временной интервал отсутствует (рис.А.2).

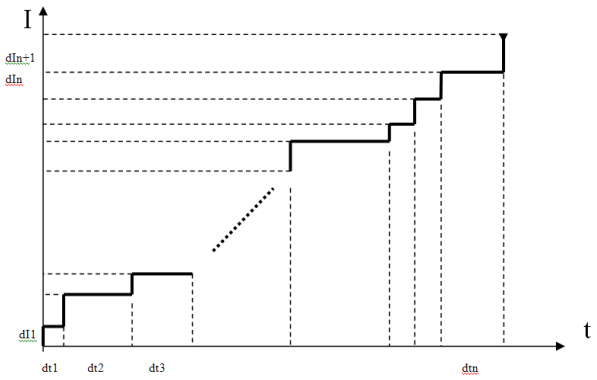


Рисунок 2 Функция распределения информации о здоровье в ИЭМК

Рассмотрение информационно-временной плоскости ИЭМК (рис.3) показывает, что при увеличении интервала времени между возникновениями двух последовательных ЭПМЗ $\Delta_1 < \Delta_2 < \Delta_3$ уменьшается угол наклона информационного вектора $\alpha_3 < \alpha_2 < \alpha_1$, что может быть использовано в качестве объективного критерия для учёта пациентов, «оторвавшихся» от диспансерного наблюдения,и организации профилактического контроля здоровья с учётом всей предыстории врачебных вмешательств.

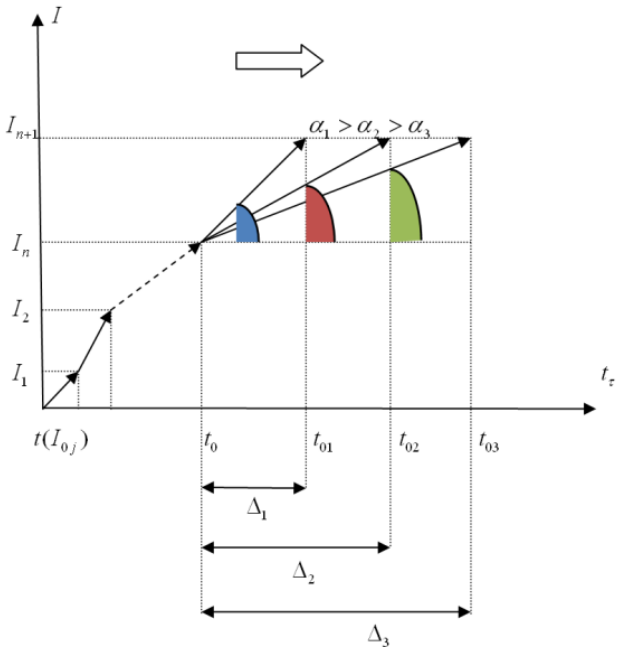


Рисунок 3. «Угол внимания» системы здравоохранения к пациенту.

В результате анализа информационного вектора ИЭМБ, может быть оценено не только его информационное наполнение (объём ресурсов здравоохранения, затраченных на пациента), но и, так называемый, «угол внимания» системы здравоохранения по отношению конкретному пациенту. Этот параметр важен при организации государственной системы диспансерного контроля состояния здоровья.

Ключевой проблемой формирования и хранения ЭПМЗ является тот факт, что до настоящего времени такой объект, как ЭПМЗ – законодательно не определён. В законе об охране здоровья нет обязательной нормы, которая всякую встречу пациента с врачом или диагностической лабораторией связывала с обязательным возникновением ЭПМЗ. Это обстоятельство существенно снижает доверие к полноте ИЭМК.

2. Идентификация электронной истории болезни и персональных электронных медицинских записей.

Именно врач принимает решение о факте рождении и смерти, поэтому можно утверждать, что система здравоохранения не нуждается в такого рода информации от отделов ЗАГС и других органов государственной власти для организации собственного документооборота. Более того, возникновение в системе новой записи $z_0(i)$ (записи о рождении), при условии централизованного учёта, может быть использовано для формирования уникального идентификатора истории болезни нового i- го пациента. Для этого достаточно использовать знания о среднем числе рождений в сутки и определить разрядность счётчика: для Петербурга достаточно трёхразрядного числа (около 150 рождений в сутки), для России в целом – четырёхразрядного счётчика (порядка 5 000 рождений), для Всемирной организации здравоохранения (ВОЗ) – семиразрядного числа.

В этом случае, уникальный идентификатор интегрированной электронной медицинской карты будет иметь вид:

<Идентификатор ИЭМК> ::= <дата рождения><учётный номер пациента> (2)

Предложенный способ идентификации (2) задаёт отношение строгого порядка на множестве ИЭМК, как в регионе, так и на федеральном уровне. Областью значений грамматической категории <Идентификатор ИЭМК> будет множество нумерованных дат рождения пациентов, а идентификатор i- го пациента – значение функции $I(z_0(i)) = I_{0i}$, для $\forall i$, где I_{0i} – уникальный идентификатор пациента, который одновременно фиксирует возраст пациента относительно текущего момента времени.

Для $\forall i, j\ I_{0i} > I_{0j}$ или $I_{0i} < I_{0j}$.

В этом случае, конечное множество идентификаторов ИЭМК ($ID = \{I_{01}, I_{02},..., I_{0n}\}$) может быть упорядочено на временной оси и интерпретироваться, как множество моментов времени, которые фиксируют события рождения пациентов. При таком подходе текущий момент времени – t_0 и идентификатор ИЭМК определяют реальный возраст пациента. Для заданного множества идентификаторов ИЭМК всегда может быть найдена карта самого возрастного пациента, не содержащая записи $z_f(i)$. Такой идентификатор обозначим как – I_{0s}.

Интервал времени $\Delta = t_0 - I_{0s}$ назовём актуальным интервалом времени жизни популяции. Ось времени, на которой размещены моменты рождения пациентов, назовём осью времени жизни популяции и обозначим – t_ρ. Ясно, что на интервале Δ зафиксированы моменты рождения не только пациентов, требующих текущего внимания системы охраны здоровья, но и тех, в истории болезни которых имеется ЭПМЗ – $z_f(i)$. Такие ЭИБ будем считать закрытыми, но не потерявшими своего информационного значения для системы здравоохранения. Обозначать такие ИЭМК будем как $\widehat{I}_{0i}$. А событие, связанное с появлением ЭПМЗ о рождении нового пациента обозначим – $\breve{I}_{0i}$.

Предложенный способ идентификации ИЭМК и её составляющих – ЭПМЗ, имеет ряд технологических преимуществ по сравнению с любым другим способом.

Психологически пациенту легко запомнить код своей электронной медицинской карты – это всего пять цифр, кроме даты рождения. Факт рождения нового пациента фиксируется именно системой здравоохранения и фиксируется раньше, чем гражданин обретает имя.

Оперативный централизованный учёт нового пациента становится реальной и просто решаемой задачей в связи с переходом на электронный документооборот в здравоохранении и созданием для этих целей федерального центра обработки данных (ЦОД).

Введение в учётную схему нового пациента любого возраста не нарушает этот строгий порядок и технологически не сложен, так как процедура связана с простым добавлением очередной записи в границах учётной даты. Таким образом, предложенный способ идентификации ИЭМК позволит однозначно связать конкретного пациента с каждой, выполненной по поводу его здоровья ЭПМЗ, с его электронной медицинской картой в конкретном лечебно-профилактическом учреждении и, наконец, с его ИЭМК в региональном и федеральном ЦОД.

Для реализации программной поддержки данного способа идентификации пациентов необходима технология идентификации ИЭМК, которая включает ряд программных агентов в федеральном ЦОД, программы идентификации и верификации имени ИЭМК пациента, работающей в каждом ЛПУ и диагностической лаборатории.

Программные агенты, поддерживающие технологию идентификации документов в базе ИЭМК ЦОД, включают:

1. Программа контроля входного потока ЭПМЗ,
2. Диалоговая программа регистрации новой ИЭМК,
3. Программа закрытия ИЭМК.

Процедура создания новой ИЭМК запускается программно по инициативе программного агента ЦОД.

3. Векторно-событийная модель базы ИЭМК.

Для построения событийной модели базы ИЭМК [3] определим ортогональную систему координат, в которой осью абсцисс станет t_ρ – дискретная ось времени жизни популяции, а осью ординат будет непрерывная временная ось, которую назовём осью времени жизни пациентов и обозначим – t_τ. Начало координат определим, как самый ранний момент времени рождения пациента, история болезни которого, по каким-то причинам, сохранилась в архивах системы здравоохранения (рис. 1), но так, чтобы все наши дальнейшие построения выполнялись в первом квадранте построенной системы координат.

Для самого возрастного пациента, идентификатор ИЭМК которого – I_{0s}, построим вектор $\vec{v}_{0s}$, длина которого $|\vec{v}_{0s}|$ будет равна реальному времени жизни этого пациента. Вектор $\vec{v}_{0s}$ разместим параллельно оси t_τ с началом в точке I_{0s}. Очевидно, что $|\vec{v}_{0s}| = \Delta$ – время жизни пациента равное времени жизни популяции.

Покажем, что вектор $\vec{v}_{0s}$ есть проекция информационного вектора истории болезни на временную ось t_τ.

Построим соответствующие вектора $\vec{v}_{0i}$ для всех учтённых ИЭМК (имеющих идентификаторы – I_{0i}), но не имеющих ЭПМЗ – $z_f(i)$. Начало этих векторов будет лежать на оси t_ρ, а конец окажется одной из точек гипотенузы равнобедренного прямоугольного треугольника с катетом $|\vec{v}_{0s}|$.

Каждый из построенных векторов суть временной образ (проекция) истории болезни конкретного пациента, который, в свою очередь, состоит из суммы векторов, число которых соответствует числу ЭПМЗ в данной ИЭМК.

$\vec{v}_{0i} = \sum_{j=1}^{k} \vec{v}_j$, где k – число записей в ИЭМК i - го пациента, а $|\vec{v}_j|$ – интервал времени от данной ЭПМЗ до следующей, либо до текущего момента t_0. Заметим, что текущий момент времени рассматриваемом в пространстве $T \times T$ характеризуется прямой $y = -t + t_0$.

Прямоугольный треугольник, катетами которого являются вектор $\vec{v}_{0s}$ и отрезок оси t_ρ – $[I_{0s}, t_0]$, ограничивает временное пространство $\Omega \subset T \times T$, в котором размещены все, без исключения, актуальные события, которые фиксируют моменты возникновения ЭПМЗ вида (1) в системе здравоохранения (системе ныне здравствующих пациентов). Актуальными будем называть такие события, которые соответствуют ЭПМЗ здравствующих пациентов, то есть пациентов, в ИЭМК которых не содержится записи – $z_f(i)$.

Таким образом, мы построили ограниченное временное пространство Ω, в котором размещены и строго упорядочены ЭПМЗ всех ныне здравствующих потенциальных пациентов (рис.А.4).

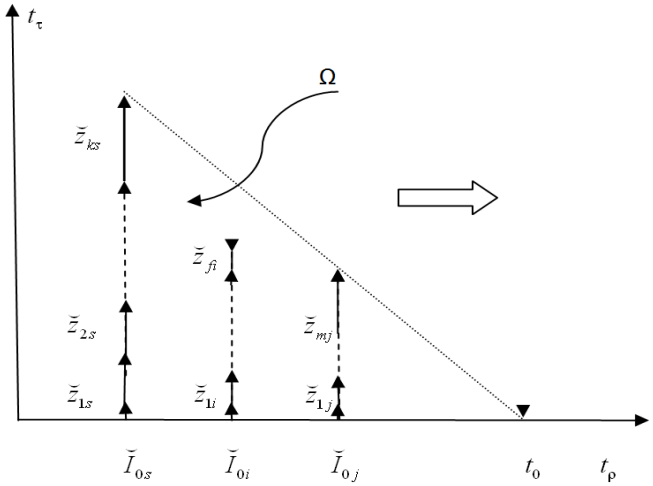


Рисунок 4. Модель событий базы ИЭМК

В данной модели для текущего момента t_0 векторные образы ИЭМК всех учтённых живых пациентов упорядочены по величине (времени жизни пациента), а вершины всех векторов лежат на одной прямой, которая является гипотенузой прямоугольного треугольника, ограничивающего временное пространство Ω. В пространстве $\Omega \subset T \times T$ размещены и строго упорядочены по оси t_ρ все ИЭМК, а по оси t_τ строго упорядочены все ЭПМЗ в векторах каждого пациента.

Гипотенуза равностороннего треугольника (пространства Ω) – это отрезок прямой $y = -t + t_0$, длиной $\sqrt{2}|\vec{v}_{0s}|$. Особенностью этого отрезка является то, что он определяет интерфейс системы здравоохранения. Именно на этом ограниченном отрезке, и только на нём, могут возникнуть новые события (ЭПМЗ) в данной модели системы охраны здоровья в текущий момент.

4. Динамика событий в модели базы ИЭМК.

Выбирая шаг h для наблюдения за динамикой развития модели событий базы ИЭМК, очевидно, речь идёт о суточном интервале, необходимо определить алгоритм учёта новых событий и исключения из рассмотрения не актуальных ИЭМК. Понятно, что правила внесения изменений в модель не должны приводить к временным коллизиям.

Пусть $h = t_1 - t_0$. Тогда, прямая $y = -t + t_0$ примет вид $y = -t + t_1 + h$, где $t_0 = t_1 + h$ текущий момент времени (рис.А.3). Прямые $y = -t + t_0$ и $y = -t + t_1$ задают временное окно, в котором разрешены новые события (возникновение новых ЭПМЗ) в системе здравоохранения. Пространство Ω потенциально увеличивается на величину $\frac{h}{2}(2\Delta + h)$.

Для приведения модели в соответствие с текущим временем t_0 должны быть выполнены следующие операции.

1. Выделение вычислительных ресурсов для ИЭМК новых пациентов, родившихся на интервале h, т.е. формирование новых идентификаторы $I_{0t_1}, I_{0t_2}, ..., I_{0t_n}$ в порядке поступления n заявок (записей $z_{0t_1}, z_{0t_2}, ..., z_{0t_n}$).

2. Для сохранения возможности фиксации точного времени новых событий в группе ИЭМК – $I_{0t_1}, I_{0t_2}, ..., I_{0t_n}$ на интервале h, соответствующие вектора назначаются равными $\vec{h}$.

3. Каждый вектор $\vec{v}_{0i}$, за исключением векторов новорождённых, увеличивается до пересечения с $y = -t + t_0$, причем если на интервале h пациент i не встречался врачом, то $\vec{v}_{0i} + \vec{h} = \vec{v}'_{0i}$ и $|\vec{v}'_{0i}| = |\vec{v}_{0i}| + |\vec{h}|$, но k – число записей в ИЭМК i - го пациента к моменту t_0 не изменяется; если на интервале h пациент i имел одну или более встреч с врачом, то $\vec{h} = \vec{v}_{0i_1} + \vec{v}_{0i_2} + ... + \vec{v}_{0i_m}$, где m – число ЭПМЗ i - го пациента на интервале h и $\vec{v}_{0i} + \vec{h} = \vec{v}'_{0i}$ и $|\vec{v}'_{0i}| = |\vec{v}_{0i}| + |\vec{h}|$, но k – число записей в ЭИБ i - го пациента к моменту t_0 увеличивается на величину m.

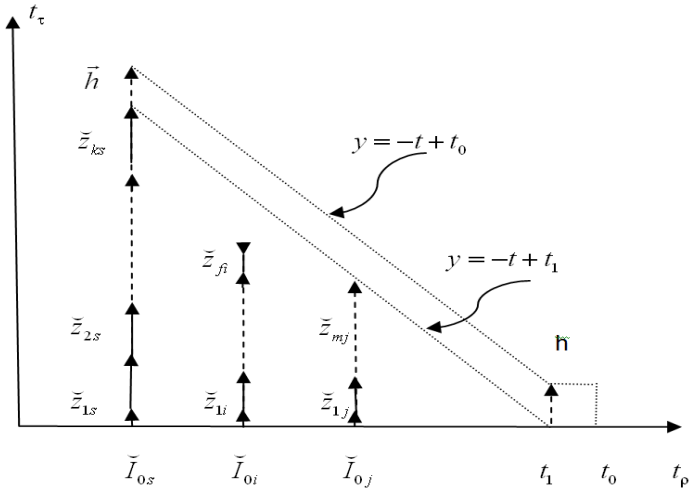


Рисунок 5 – Динамика событий в модели базы ИЭМК

4. Если на интервале h у i- го пациента возникает запись $z_f(i)$ (вектор – $\vec{v}_{fi}$), то ИЭМК закрывается, обозначим её как $I_{0i} = [I_{0i}]$, а вектор $\vec{v}_{0i}$ обращается в скаляр $|\vec{v}'_{0i}| = |\vec{v}_{0i}| + |\vec{v}_{fi}|$.

5. Если на интервале h у S - го пациента (самого возрастного) возникает запись $z_f(i)$, то выполняется коррекция (уменьшение) пространства Ω. Для этого в списке идентификаторов ИЭМК

определяется такой не закрытый I_{0i}, что $\Delta = t_0 - I_{0i} = \max$. Для выбранного идентификатора ИЭМК I_{0i} фиксируется статус I_{0s}.

6. Вычисляются характеристики пространства Ω на момент времени t_0 :

– число актуальных историй болезни (число живых пациентов);

– число закрытых ИЭМК на интервале h (число умерших в текущие сутки);

– коэффициент выживаемости для пространства Ω, а также для любой заданной возрастной категории пациентов (отношение числа актуальных ИЭМК к общему числу учтённых ИЭМК);

– и т.д., и т.п.

Рассмотренный алгоритм указывает на то, что формирование полной, достоверной и доступной для обработки базы ИЭМК предполагает наличие нового класса программных агентов, выполняющих непрерывное обслуживание потока ЭПМЗ в региональных и федеральном ЦОД.

В состав этих агентов с необходимостью входят:

1. Программа контроля разрешённого интервала изменений,
2. Программа коррекции пространства событий
3. Программа коррекции информационного вектора ИЭМК при отсутствии событий на данном интервале.
4. Программа расчёта статистических данных на заданном интервале
5. Программа коррекции интегральных статистических характеристик актуального пространства событий.
6. Программа коррекции актуального списка пациентов.

5. Информационная модель базы ИЭМК.

Интегрированная электронная медицинская карта - это сумма векторов – ЭПМЗ, которая дополняется системой охраны здоровья на протяжении всей жизни пациента. Начиная с момента рождения, система здравоохранения производит персональные медицинские записи (теперь – ЭПМЗ) и последовательно размещает их в истории болезни (теперь – ИЭМК). Каждая запись имеет собственное информационное наполнение. Не пытаясь на этом этапе оценивать семантику записи, мы всегда можем посчитать количество бит, необходимых для хранения данной ЭПМЗ в памяти компьютера. Ясно, что каждый бит такой записи, в той или иной степени несёт в себе информацию о ресурсах, затраченных системой здравоохранения на данного пациента. Очевидно, что каждый вектор (ЭПМЗ) имеет фиксированную по величине (количеству бит) проекцию на информационно-временную плоскость $I \times T_\rho$ (см. рис. 6).

Особенность предлагаемой информационной модели базы ИЭМК заключается в том, что, при сохранении неизменной величины проекции вектора ЭПМЗ на плоскость $I \times T_\rho$ (в записи не добавляется битов), его проекция на плоскость $I \times T_\tau$ непрерывно увеличивается до момента появления очередной ЭПМЗ, что характеризует процесс старения информации.

Вектор последней записи (ЭПМЗ) будет изменять величину и угол наклона к плоскости $I \times T_\tau$ вплоть до появления очередной записи.

Каждая ИЭМК размещена в персональной для данного пациента информационно-временной плоскости ($I \times T$), которая характеризуется моментом рождения – I_{0i} (рис.3).

Информационная составляющая ЭПМЗ является объектом семантического анализа и предполагает наличие нового класса программных агентов для оперативной оценки эффективности использования ресурсов здравоохранения и раннего обнаружения дефектов оказания медицинской помощи в результате обработки полной, достоверной и доступной для автоматизированной обработки информации в базе ИЭМК.

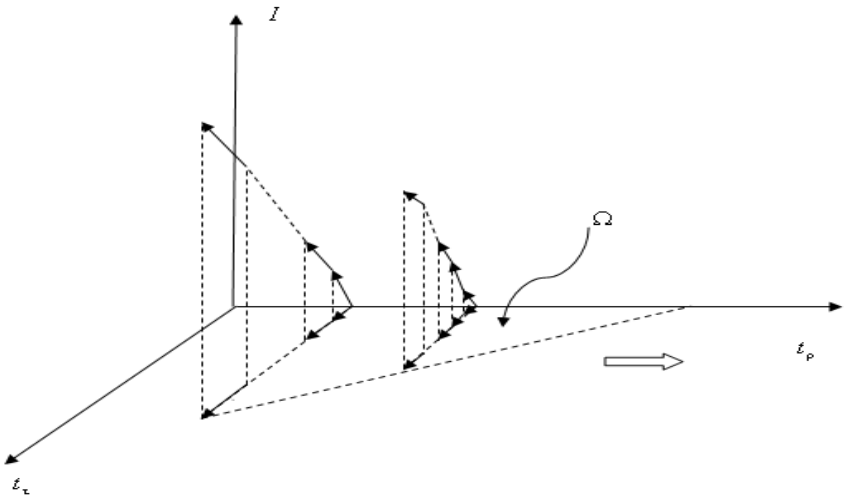


Рисунок 6 – Информационная модель базы ИЭМК

6. Мониторинг состояния системы здравоохранения по модели базы ИЭМК.

Анализ формальной событийной модели базы ИЭМК, которая нацелена на хранение полного, достоверного и доступного для автоматизированной обработки потока первичной медицинской информации, указывает на то, что для функционирования и эффективного использования этой базы данных с необходимостью должны быть реализованы взаимообусловленные коллекции программных агентов, то есть программы, которые выполняют непрерывный мониторинг состояния базы ИЭМК и поддерживают её функционирование.

Важной особенностью предложенной модели являются три эквивалентные способа визуализации текущего момента времени: во-первых, как точки на временной оси, во-вторых, как ограниченной прямой – гипотенуза прямоугольного треугольника (см. рис. А.4) и, в третьих, в виде ограниченной плоскости, проходящей через гипотенузу треугольника событий и перпендикулярной плоскости $\Omega \subset T \times T$ (рис.А.6).

Линейная форма фиксации текущего момента времени позволяет визуализировать всех наблюдаемых пациентов с учетом их возраста.

Фиксация момента времени в виде плоскости позволяет визуализировать всех наблюдаемых пациентов не только с учётом возраста, но и с учётом ресурсов, затраченных системой здравоохранения.

Можно показать, что любого момента времени «плоскость момента времени» (ПМВ) в нашей модели ограничена по оси абсцисс отрезком временной оси равным произведению возраста самого старшего пациента на корень квадратный из двух – Ts *√2, а по оси ординат максимальной величиной информации, содержащейся в одной ИЭМК.

Результат мониторинга состояния пациентов на любом их трёх выше указанных уровней системы охраны здоровья может отображаться точками на ПМВ. Положение точки на плоскости характеризуется двумя параметрами: возрастом пациента и количеством информации в его ИЭМК (объёмом ресурсов, затраченных системой здравоохранения на данного пациента). (рис. 7).

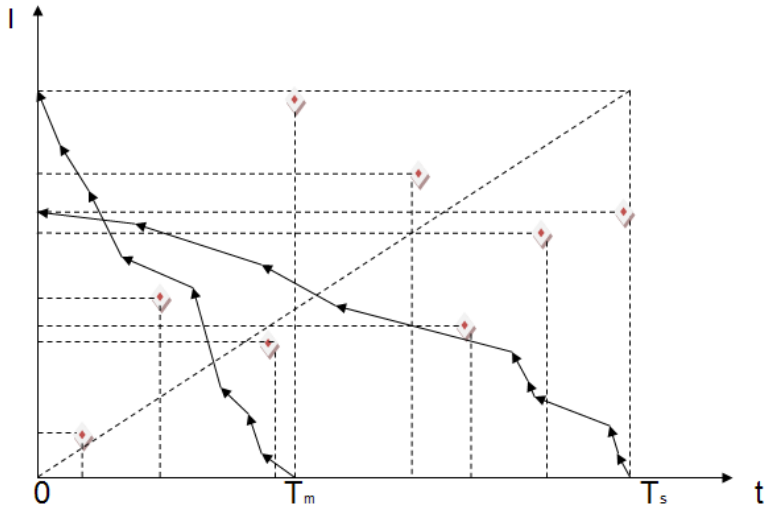


Рисунок 7. Мониторинг базы ИЭМК – плоскость момента времени

На рис. 7 представлены точки, которые отражают объём информации в ИЭМК пациентов различных возрастов. Для двух пациентов (самого возрастного и самого «информативного») приведены следы векторных моделей их ИЭМК.

Можно доказать, что плоскости мониторинга различных регионов могут суммироваться, что не приведёт к коллизии данных, так как на множестве ИЭМК задано отношение строгого порядка.

Свойства ПМВ далеко не исследованы, что требует специальных усилий в рамках проекта цифровизации здравоохранения

7. Выводы.

Разработанная динамическая модель потока первичной медицинской информации в клинической сфере здравоохранения представляет полный, достоверный и доступный для автоматизированной обработки набор данных с целью информационной поддержки врачебной деятельности и раннего обнаружения дефектов оказания медицинской помощи, то есть повышения информационной безопасности пациентов.

Важным шагом на пути внедрения такой модели в практику здравоохранения должна стать фиксация в законе такого объекта как ЭПМЗ и директивное направление потока ЭПМЗ в федеральный ЦОД. Эти цели могут быт достигнуты, например, внесением изменений в ФЗ № 326-ФЗ.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И.В., Саенко И.Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. № 3 (22). СПб.: Наука, 2012. С.84-100.
2. Браницкий А.А., Котенко И.В. Открытые программные средства для обнаружения и предотвращения сетевых атак (окончание) // Защита информации. Инсайд. — 2017. — 3 (75). — С. 58–66.

УДК004.056

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ НСД С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ОЦЕНКИ И АНАЛИЗА ЭМОЦИОНАЛЬНОЙ ЭКСПРЕССИИ И МИМИКИ ПОЛЬЗОВАТЕЛЯ

Брагина Елизавета Константиновна, Егоров Илья Эдуардович
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: AlisBrain@mail.ru, mynameisiliaegorov@gmail.com

Аннотация. В статье *и*сследуется проблема минимизации возможности получения несанкционированного доступа к информационным системам, в которых хранится и обрабатывается информация ограниченного доступа. Рассматривается метод биометрической аутентификации основанный на оценке эмоциональной экспрессии и мимики идентифицируемого пользователя путем постоянного скрытого мониторинга при помощи web-камеры. Приводится определение эмоций, анализируются методы определения эмоции по выражению лица, используемые экспертами. Сделан вывод о необходимости автоматизации процесса распознавания эмоций по выражению лица и мимике исследуемого человека. Охарактеризованы и проанализированы современные системы распознавания эмоций и методы машинного обучения. По результатам анализа для увеличения точности распознавания эмоций в алгоритме работы данных систем предложено использовать методы системы кодирования активности лицевых мышц, адаптированные для использования машиной и методы машинного обучения.

Ключевые слова: *информационные системы; информационная безопасность; биометрическая аутентификация; распознавание эмоций; система кодирования активности лицевых мышц; технологии машинного обучения.*

INCREASING THE PROTECTION OF INFORMATION FROM UNAUTHORIZED ACCESS USING BIOMETRIC AUTHENTICATION

Bragina Elizaveta, Egorov Ilia
St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Kronverksky pr., 49, St. Petersburg, Russia
e-mails: AlisBrain@mail.ru, mynameisiliaegorov@gmail.com

Abstract. The article explores the problem of minimizing the possibility of obtaining unauthorized access to information system in which restricted information is stored and processed. The method of biometric authentication based on the evaluation of emotional and face expressions of an identified user is being considered by means of constant hidden monitoring with help of web camera. The definition of emotions is given, methods for determining emotion by facial expressions, used by experts, are analyzed. The conclusion is made about the necessity of the automation the process of recognizing emotions by expressing the face and facial expressions of the person being studied. Characterized and analyzed modern

systems of recognition of emotions and methods of machine learning. Based on the results of the analysis, to increase the accuracy of the recognition of emotions in the algorithm of the operation of these systems, it is proposed to use methods of the coding system for the activity of facial muscles, adapted for use by the machine and methods of machine learning.

Keywords: *information systems; information security; biometrical authentication; emotion recognition; system of coding facial muscles; machine learning technologies.*

Введение.

В наше время неотъемлемой частью всевозможных сфер повседневной деятельности человека стало использование информационных систем (далее – ИС). ИС используются для хранения, обработки и поиска информации, в том числе и информации ограниченного доступа. Право доступа к данной информации ограничено установленными законами, нормами и правилами [1], поэтому существует потребность в обеспечении её информационной защищенности, а, следовательно, и информационной защищенности ИС.

Достижение состояния защищённости информации в ИС обеспечивается созданием комплексной системы защиты, одной из главных составляющих которой являются методы защиты от несанкционированного доступа (далее – НСД).

Основой программно-технических средств защиты от НСД являются процедуры идентификации (пользователь называет себя) и аутентификации (проверки подлинности) пользователей [2].

Существуют три типа метода аутентификации, однако первые два типа, которые являются более традиционными для современного человека, процедуры аутентификации (основанные на знании чего-либо, на владении чем-либо) имеют существенные недостатки, такие как: простота подбора, риск кражи или утери, копирование и т.д. Третий метод (основанный на части самого пользователя) – биометрическая аутентификация или аутентификация на основе биометрических характеристик (далее – БХ) имеет следующие преимущества:

– БХ удобно использовать благодаря отсутствию необходимости контакта;

– БХ невозможно потерять или забыть, т. к. они являются частью идентифицируемого пользователя (далее – ИП);

– значительно затруднены передача и подделка БХ.

Проанализировав современные методы биометрической аутентификации можно смело сказать то, что метод, основанный на оценке эмоционального состояния и мимики, является наиболее перспективным, т. к. его использование снижает вероятность возникновения ошибок первого и второго рода, тем самым повышая защищенность ИС [3].

Рассматриваемый авторами метод биометрической аутентификации основан на оценке эмоциональной экспрессии и мимики ИП путем постоянного скрытого мониторинга при помощи web-камеры.

Алгоритм данного метода описан далее.

Шаг 1. Создание базы данных личных карточек пользователей.

В личных карточках пользователей должна храниться информация об исследовании эмоциональной экспрессии и мимики ИП во время повседневной работы в ИС, а именно: атласы фотоизображений (размеченные фотографии ИП), основные характеристики динамики эмоциональной экспрессии, результаты определения эмоций и анализ эмоционального состояния с учетом влияния внешних факторов.

Шаг 2. Распознавание эмоций ИП в динамической форме.

Распознавание эмоций ИП в динамической форме осуществляется посредством web-камеры с достаточным уровнем характеристик (тип матрицы, разрешение, оптика, чувствительность матрицы и т.д.), установленной на автоматизированном рабочем месте.

Шаг 3. Сравнение результатов шага «2» с базой данных, созданной на шаге «1».

Под сравнением следует понимать выявление отклонений результатов постоянного определения эмоций от эталонов, хранящихся в базе данных.

Шаг 4. Анализ результатов сравнения.

Последующий анализ данных отклонений заключается в определении возможности возникновения инцидента (на данном шаге система определяет возможность несанкционированных действий пользователя).

Шаг 5. Предпринятие соответствующих действий/мер.

Далее система должна предпринять соответствующие действия/меры, например, подать предупреждающий сигнал на пост охраны.

Эмоции. Методики определения эмоций по выражению лица.

Эмоции – это особая формапсихических процессов или состояний человека, которые в форме непосредственного переживания отражают субъективное отношение (радость, страх, удивление и

т.д.) к объективным явлениям окружающего мира и событиям, происходящим в течение жизни человека.

Главные особенности эмоций состоят в том, что они:

- выражают значимость действующих на человека объектов и ситуаций;
- возникают спонтанно;
- зависят от внешних факторов.

Выделяются следующие функции эмоций: отражательная, побуждающая, подкрепляющая, переключательная, коммуникативная. Отражательная или оценочная функция проявляется в обобщенной оценке событий. То есть эмоции охватывают человека и тем самым производят обобщение всех видов выполняемой им деятельности. В рамках побуждающей функции рассматривают два класса эмоций: ведущие и производные.

Ведущее эмоциональное состояние, направленное на предмет – цель человека, инициирует характерное поведение. Производное эмоциональное состояние возникает в результате анализа своего поведения и побуждает человека действовать в прежнем направлении или менять поведение. Подкрепляющая функция эмоций выражается в непосредственном участии в процессах обучения и памяти. Переключательная функция обнаруживается в ситуации возникновения конкуренции между мотивами действия. Коммуникативная же функция заключается в том, что благодаря мимике и выражению лица человек передаёт своё эмоциональное состояние окружающим его людям и происходит это, как правило, не осознанно.

Эмоции выражаются не только в двигательных реакциях, но и в уровне тонического напряжения мышц. При этом эмоции непосредственно связаны с функциями определенных структур мозга, то есть эмоции человека имеют прямую зависимость от внутренней среды мозга. Следовательно, на лице человека, который замыслил некоторое «злодеяние», проявятся эмоциональная экспрессия и мимика, выдающие соответствующие испытываемые эмоции [4].

На сегодняшний день, основными методиками определения эмоций по мимике и выражению лица являются: идентификация эмоций по выражению лица (Facial Affect Scoring Technique – FAST) и система кодирования активности лицевых мышц (Facial Action Coding System – FACS).

FAST – это метод кодирования мимических выражений, основанный на сравнении исследуемого лица с некоторым атласом фотоэталонов. Фотоэталон состоит из трех частей, соответствующих трем уровням лица: лбу, глазам и нижней части. При этом атлас фотоэталонов существует для каждой из базовых эмоций, такими эмоциями являются: радость, удивление, грусть, страх, гнев и отвращение. Использовать данный метод возможно только при исследовании эмоции, находящейся в статической форме, т.е., например, на фотографии – это является существенным неудобством [5].

Системой, фиксирующей не только общий внешний вид выражений лица, но и замечающей моменты начала, кульминации и исчезновения активности лицевых мускулов, учитывающей временные характеристики и показатели интенсивности является система кодирования активности лицевых мышц, или FACS. В данной системе основными единицами измерения являются видимые, едва различимые изменения тонуса лицевых мышц. При этом эксперт, зная все возможные варианты движения мускулов с точки зрения функциональной анатомии лица, сопоставляет их с кодами двигательных единиц, оценивает интенсивность и симметричность и в итоге определяет какую из основных эмоций, испытывает исследуемый человек. Отмечается что, данный метод предназначен для использования именно человеком-экспертом [6]. Целью данных исследований и обучений экспертов является не только прямое распознавание эмоций, но и выявление тех эмоций, которые тщательно пытается скрыть исследуемый. Исходя из конкретных ситуаций, с помощью системы кодирования FACS выявляют, например, преступников. Это стало причиной сотрудничества экспертов с судьями, адвокатами и полицейскими, а также со специальными службами.

Естественно, таких экспертов, которые безошибочно определяют эмоции, видят скрытые эмоции и определяют лжецов не так много, как ситуаций, в которых их способности могли бы стать очень полезными. Данную проблему смогла бы разрешить автоматизация процесса, однако для этого необходимо приспособить систему FACS для использования её машиной.

Системы распознавания эмоций по выражению лица.

Система распознавания эмоций по выражению лица – это автоматизированная система, предназначенная для определения базовых эмоций человека на фотографии или видеозаписи по мимике и лицевой экспрессии.

Современные системы распознавания эмоций работают по следующему общему алгоритму:

1. распознавание лица;
2. обработка лица;
3. анализ;
4. выдача результата.

То есть основными различиями данных систем является выбор определенных методов как для распознавания лица и обработки, так и для непосредственного определения эмоций.

При этом практически все системы в результате выводят список основных эмоций (радость, удивление, грусть, страх, гнев и отвращение) с процентным соотношением преобладания каких-либо из них на обрабатываемом изображении.

В настоящее время по большей части данные автоматизированные системы используются для маркетинговых исследований, а также просто для развлечения людей.

Главная характеристика оценивания данных систем – это точность определения эмоций. Вычислить данную величину возможно исключительно при проведении практических исследований. По данным разработчиков современных систем, она колеблется от 80-90%, что является не стабильным и не достаточным результатом для использования данных систем с целью, например, неоспоримого определения «злоумышленника» [7].

Технологии машинного обучения.

Интеллектуальный агент – это система, которая способна воспринимать определенную среду с помощью датчиков и воздействовать на неё с помощью исполнительных механизмов. Схема работы и взаимодействий агента представлена на рис. 1.

В рассматриваемой теме в качестве входных данных (восприятие) агент должен получить: фотоизображения, основные характеристики динамики эмоциональной экспрессии, а также информацию о внешней среде. Его воздействие (действия) на среду будет выражаться либо в бездействии и продолжении работы, либо в выведении предупреждающего сообщения на монитор охраны, специалистов по информационной безопасности, руководителя отдела и т.п.

Поведение интеллектуального агента описывается с помощью функции агента, которая отображает любую последовательность актов восприятия на некоторое действие. Под последовательностью актов восприятия следует понимать полную историю всего, что было когда-либо воспринято агентом. При этом реализация функции происходит с помощью программы агента. То есть функция – это математическое описание, а программа – это конкретная реализация [8].

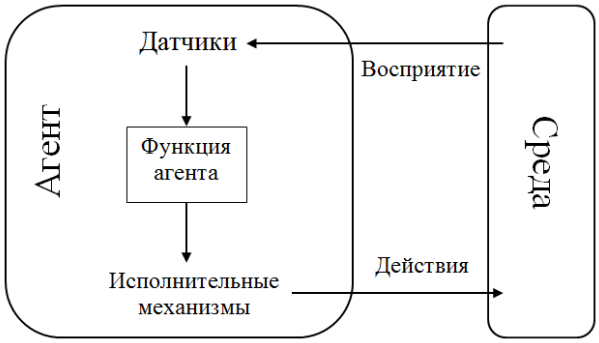


Рис. 1. Работа и взаимодействия агента

Для достижения рациональности или «правильности» агент должен не только собирать информацию, но и обучаться в максимально возможной степени на тех данных, которые он воспринимает.

Машинное обучение – это процесс модификации компонентов агента для достижения улучшения производительности. То есть, средства машинного обучения позволяют агенту приспосабливаться к новым обстоятельствам, а также обнаруживать и распространять признаки стандартных ситуаций.

Общими компонентами обучающегося агента являются:

– обучающийся компонент – отвечает за внесение модификаций;
– производительный компонент – обеспечивает выбор внешних действий;
– критик – выполняет оценку действий агента;
– генератор проблем – производит всевозможные исследовательские действия.

Структура компонентов и их способы представления во многом зависят от конкретного назначения интеллектуального агента, соответственно разнообразие методов обучения крайне велико. Однако абсолютно все методы объединены тем, что сам процесс обучения заключается в модификации каждого компонента агента.

Следовательно, с помощью машинного обучения агент сможет улучшать навыки анализа входных данных и соответственно в рассматриваемом случае увеличивать точность определения эмоций до максимально возможных 97,5% [7].

Заключение. Таким образом, для эффективной работы и увеличения точности автоматизированных систем распознавания эмоций (повышения качества распознавания эмоций) до 95-97,5% авторами предлагается использовать методы системы кодирования активности лицевых мышц, адаптированные для использования машиной и методы машинного обучения в алгоритме работы данных систем.

С применением предложенных методов система распознавания эмоций в идеале должна будет:

– обладать достаточными умениями для распознавания эмоций с точностью в 95-97,5%;
– анализировать полученные данные;
– на выходе, производить какие-либо действия, исходя из полученных результатов анализа.

Всё вышесказанное позволит использовать системы распознавания эмоций для обеспечения защиты информации в ИС.

СПИСОК ЛИТЕРАТУРЫ

1. Домарев В. В. Безопасность информационных технологий. Системный подход //К.: ООО ТИД Диа Софт. – 2004.
2. Методы и средства защиты от несанкционированного доступа // URL: http://www.panasenko.ru/Articles/77/77.html (дата обращения: 11.03.2017).
3. Брагина Е.К., Соколов С.С. Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития. – Вестник Астраханского государственного технического университета. – 2015. – №. 1.
4. Хомская Е. Д. ББК 28.707 я73:© Данилова НН, Крылова АЛ, 2005© Оформление. Изд-во «Феникс», 2005 //update. – 2005. – Т. 27. – С. 06.
5. Диагностика психического состояния человека по мимике лица // URL: http://meddoc.com.ua/diagnostika-psihicheskogo-sostoyaniya-po-mimike-lica/ (дата обращения: 10.03.2017).
6. Трусов В. П. Выражение эмоций на лице (по материалам работ П. Экмана) //Вопросы психологии. – 1982. – Т. 1. – №. 982. – С. 144-147.
7. Брагина Е.К., Егоров И.Э. Современные системы распознавания эмоций по выражению лица: обзор, анализ и определение перспектив развития. – IT: ВЧЕРА, СЕГОДНЯ, ЗАВТРА: материалы V научно-практической конференции студентов, аспирантов и курсантов ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» – СПб.: Изд-во ГУМРФ им. адм. С.О. Макарова, 2017 – С. 13-21.
8. Рассел С., Норвиг П. Искусственный интеллект: современный подход //физика. – 2006. – Т. 537. – №. 322. – С. 3.

УДК 004.056

СЕТЕВЫЕ АТАКИ СО СКРЫТИЕМ И СО ВСТАВКОЙ НА ПРИМЕРЕ SNORT, SURICATA И BRO

Браницкий Александр Александрович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mail: branitskiy@comsec.spb.ru

Аннотация. В докладе представлено экспериментальное исследование трех сетевых систем обнаружения атак (СОА): Snort, Suricata и Bro. Основной целью является выявление слабых мест в реализации их сетевого стека при помощи тестовых последовательностей пакетов, позволяющих выполнять обманные приемы уклонения от сигнатурных правил. Раскрывается понятие двух типов сетевых атак, которым подвержены исследуемые СОА. Описывается разработанный программный инструмент для проведения экспериментов.

Ключевые слова: *сетевые атаки со скрытием; сетевые атаки со вставкой; сетевой стек.*

EVASION AND INSERTION NETWORK ATTACKS ON THE EXAMPLE OF SNORT, SURICATA AND BRO

Alexander Branitskiy
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
e-mail: branitskiy@comsec.spb.ru

Abstract. The report presents an experimental investigation of three network attack detection systems (ADSs): Snort, Suricata and Bro. The main purpose is to identify weaknesses in the implementation of their network stack using the test sequences of packets which allow to perform elusion fraudulent approaches of signature rules. The concepts of two types of network attacks are revealed to which the investigated ADSs are exposed. The developed software tool for carrying out the experiments is described.

Keywords: *evasion network attacks; insertion network attacks; network stack.*

Сетевые атаки как один из способов нарушения безопасности в компьютерной сети являются предметом острых дискуссий среди работников и научной, и технической сфер деятельности. Вопросы построения защищенных систем, подключенных к сети Интернет, являются актуальными, и одним из наиболее известных подходов, направленных на их решение, является использование сигнатурных СОА [1]. В то же время даже эти программные компоненты подвержены некоторым

видам сетевых атак. В настоящем докладе предлагается рассмотреть различные сетевые атаки, которые позволяют “ввести в заблуждение” сигнатурные правила СОА, и предложить несколько практических рекомендаций для избежания возникновения таких случаев.

Сетевые атаки со скрытием и со вставкой. Для обхода сигнатурных правил СОА можно выделить два варианта.

(1) Для атак со скрытием пакет, содержащий потенциально вредоносный контент, формируется таким образом, чтобы СОА не реагировала на него, а сетевой стек защищаемой ОС воспринимал его как часть некоторой TCP-сессии. Этот случай является наиболее пагубным для целевого хоста и приводит к пропуску атаки.

(2) Для атак со вставкой наблюдается противоположная ситуация: мошенник подбирает такую последовательность TCP-пакетов, чтобы в сетевом стеке СОА они собирались в требуемом порядке, а на целевом хосте — с игнорированием определенных пакетов. Применение таких атак, как правило, приводит к ложным срабатываниям. Фундаментальной работой в области исследования таких атак является [2]. Рекомендации для противодействия атакам со скрытием и со вставкой могут включать как настройку межсетевого экрана для принудительного отбрасывания фрагментированных на уровне IP пакетов, так и замену сигнатурных СОА их хостовыми аналогами.

Эксперименты. Для проведения экспериментов был разработан программный инструмент, выполняющий функции асинхронного проксирования TCP-соединений с возможностью генерации компрометирующих сетевой стек СОА или ОС последовательностей пакетов [3]. Данное программное средство обладает клиент-серверной архитектурой и предоставляет сетевые услуги как анонимного сокрытия IP-адреса источника генерации атак, так и видоизменения некоторых переадресуемых от него пакетов. Разработанные сценарии атак покрывают четыре уровня модели OSI и включают такие преобразования, как разбиение TCP-пакетов на несколько фрагментов, отправка TCP-пакета с выдержанной паузой и пр. Алгоритм обработки множественных подключений от разнородных клиентов оптимизирован особым образом, что позволяет избавиться от порождения нового процесса, предназначенного для поддержания установленного между сервером и клиентом соединения.Запросы, поступающие от тонких клиентов, например wget и ftp, претерпевают ряд изменений согласно заранее определенным пользователем сценариям, которые описывают сетевые атаки со скрытием и со вставкой. Тестовый макет включает в себя три виртуальные машины с различными ОС. Одна из них предназначена для создания TCP-сессий с поддельными пакетами, на остальных установлены исследуемые СОА: Snort, Suricata и Bro. Результаты выполненных экспериментов показывают, что сетевой стек каждой рассмотренной СОА подвержен нескольким выявленным уязвимостям.

В докладе исследованы три СОА с точки зрения их способности справляться с обработкой последовательностей TCP-пакетов, возможно, приводящих к обходу сигнатурных правил. Выполнены эксперименты, нацеленные на тестирование исследуемых СОА. Направление дальнейших исследований может включать как расширение списка исследуемых СОА, так и добавление новых сценариев атак со скрытием и со вставкой.

Благодарности. Работа выполнена при финансовой поддержке РФФИ (проекты 15-07-07451, 16-37-00338) и № 0073-2015-0004 и 0073-2015-0007 в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И.В., Саенко И.Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. № 3 (22). СПб.: Наука, 2012. С.84-100.
2. Ptacek T.H., Newsham T.N. Insertion, evasion, and denial of service: Eluding network intrusion detection: tech. rep. / SECURE NETWORKS INC CALGARY ALBERTA. — Jan. 1998.
3. Браницкий А.А., Котенко И.В. Открытые программные средства для обнаружения и предотвращения сетевых атак (окончание) // Защита информации. Инсайд. — 2017. — 3 (75). — С. 58–66.

УДК 004.056

АЛГОРИТМЫ ПАРАЛЛЕЛЬНОГО ПОИСКА ШАБЛОННЫХ ПОДСТРОК ПРИ РЕАЛИЗАЦИИ СИГНАТУРНЫХ ПРАВИЛ СОА

Браницкий Александр Александрович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mail: branitskiy@comsec.spb.ru

Аннотация. В докладе представлено экспериментальное исследование трех алгоритмов поиска шаблонных подстрок: алгоритма Ахо–Корасик, алгоритма Бойера–Мура и инкрементального алгоритма. Основной целью является повышение скорости обработки содержимого в сетевых пакетах. В рамках доклада предлагается рассмотреть несколько параллельных модификаций представленных алгоритмов. Описываются результаты выполненных экспериментов с использованием сигнатурных правил Snort.

Ключевые слова: *сигнатурные правила; системы обнаружения атак; поиск подстрок.*

ALGORITHMS FOR PARALLEL SEARCHING OF TEMPLATE SUBSTRINGS IN REALIZATION OF ADSSIGNATURE RULES

Alexander Branitskiy
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
e-mail: branitskiy@comsec.spb.ru

Abstract. The report presents an experimental investigation of three algorithms for searching of pattern substrings: the Aho–Corasick algorithm, the Boyer–Moore algorithm, and the incremental algorithm. The main purpose is to increase the rate of processing the content in network packets. Within the report it is proposed to consider several parallel modifications of the presented algorithms. The results of performed experiments using Snort signature rules are described.

Keywords: *signature rules; attack detection systems; substring search.*

С ростом объема передаваемой в сети Интернет информации возникают вопросы, связанные с необходимостью быстрой проверки этих данных на предмет наличия в них содержимого, вредоносного для оконечных пользовательских устройств, серверов и промежуточных маршрутизирующих узлов. Вставка управляющих символьных последовательностей, содержащих команды исполнения сценариев оболочки, может приводить к запуску вредоносных процессов с правами суперпользователя (к примеру, через Web- или SQL-сервер). Для выявления и предотвращения попыток подобных несанкционированных действий предназначены СОА. Однако эффективность реализованных в них алгоритмов сигнатурного сопоставления с образцом требует совершенствования. В настоящем докладе для решения этой задачи предлагается использовать аппаратные ускорители: ядра центрального процессора (CPU)и графической видеокарты (GPU).

Параллельные алгоритмы поиска шаблонных подстрок. При разработке алгоритмов поиска шаблонных подстрок использовались две параллельные модификации. (1) Алгоритм Ахо–Корасик [1]подразумевает построение конечного автомата, в котором состояния-узлы рассматриваются как позиции из набора шаблонных подстрок, а условием смены состояний является совпадение текущего символа из анализируемой строки с очередным символом из шаблонной подстроки. В то время как в стандартном исполнении алгоритма стартовой точкой при сканировании входной строки является ее первый символ, в параллельной модификации этого алгоритма предлагается разбить входную строку на несколько подстрок, каждой из которых будет назначена независимая копия построенного автомата в отдельном потоке. Поскольку неизбежны случаи, в которых отдельные части искомой подстроки могут встречаться в смежных позициях из разных разбиений, выполненных для анализируемой строки, то при разработке модифицированной таким образом версии алгоритма необходимо отслеживать изменения глубин в дереве-автомате во время смены состояний. (2) Алгоритм Бойера–Мура [1] при сканировании входной строки выполняет переменный сдвиг шаблонной подстроки, который зависит от количества успешно сопоставленных символов, встречающихся в суффиксе подстроки. Разработанная модификация данного алгоритма направлена на разбиение множества искомых подстрок на несколько непересекающихся частей и выполнение поиска каждого элемента образовавшегося набора внутри отдельного потока. Такой подход характеризуется простотой реализации и демонстрирует существенный выигрыш в случаях большого размера набора шаблонных подстрок.

Эксперименты. Для выполнения экспериментов был разработан генератор символьных последовательностей [2], который позволяет формировать тестовые наборы анализируемых строк на основе сигнатурных правил Snort. Экспериментальное сравнение осуществлялось для трех алгоритмов: алгоритма Ахо–Корасик, алгоритма Бойера–Мура и алгоритма инкрементального поиска. В результате выполненных экспериментов было определено, что наилучшими показателями обладает алгоритм Ахо–Корасик. Параллельные модификации первых двух алгоритмов были реализованы с использованием технологий OpenMPи CUDA, предназначенных для создания многопоточных приложений с распараллеливанием на уровне ядер CPU и GPU соответственно. Использование параллельных алгоритмов позволило добиться увеличения скорости обработки шаблонного сопоставления с образцом более чем в 1.5 раза на уровне CPUи более чем в 1000 раз на уровне GPUдля случая алгоритма Ахо–Корасик, а также более чем в3 раза на уровне CPUи более чем в 3000 раз на уровне GPUдля случая алгоритма Бойера–Мура.

В докладе исследованы три алгоритма шаблонного поиска подстрок. Рассмотрены параллельные модификации алгоритмов Ахо–Корасик и Бойера–Мура, выполнены эксперименты. Направление дальнейших исследований включает разработку других алгоритмов параллельного поиска подстрок.

Благодарности. Работа выполнена при финансовой поддержке фонда содействия развитию малых форм предприятий в научно-технической сфере (договор № 9167ГУ/2015 от 24.12.2015).

СПИСОК ЛИТЕРАТУРЫ

1. Aho A. V. Algorithms for finding patterns in strings // Handbook of Theoretical Computer Science. Algorithms and Complexity. — 1990. — Pp. 255–300.

2. Браницкий А.А. Архитектура распределенной системы обнаружения, классификации и предотвращения сетевых атак на основе сигнатурного анализа и методов вычислительного интеллекта // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016), 2016. — С. 651–655.

УДК 004.056

КЛАССИФИКАЦИОННЫЕ ПРИЗНАКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ VANET[1]

Буйневич Михаил Викторович, Столярова Екатерина Сергеевна, Хорошенко Сергей Викторович,
Ширяев Денис Михайлович, Владыко Андрей Геннадьевич
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
Россия, Санкт-Петербург, пр. Большевиков, 22, корп. 1
e-mails: bmv1958@yandex.ru, ekaterinastoljarova@rambler.ru, khoroshenko@sut.ru,
shiryaev.dm@spbgut.ru, vladyko@sut.ru

Аннотация. В докладе проведен критический анализ подходов к классификации угроз информационной безопасности автомобильных беспроводных сетей (VANET).

Ключевые слова: *VANET; информационная безопасность; угроза; классификационные признаки.*

CLASSIFICATION FEATURES OF INFORMATION SECURITY THREATS IN VANET

Mikhail Buinevich, Ekaterina Stolyarova, Sergei Khoroshenko, Denis Shiryaev, Andrei Vladyko
Bonch-Bruevich St. Petersburg State University of Telecommunications
Russia, St. Petersburg, Bolshevikov pr., 22/1
e-mails: bmv1958@yandex.ru, ekaterinastoljarova@rambler.ru, khoroshenko@sut.ru,
shiryaev.dm@spbgut.ru, vladyko@sut.ru

Abstract. The approaches to information security threats classification of VANET, the most common sources, are critically examined.

Keywords: *VANET; information security; threat; classification features.*

Сети VANET (от англ. vehicular ad hoc network – автомобильные беспроводные сети) – это передовые инфокоммуникационные технологии, нацеленные на обеспечение повышения безопасности и эффективности дорожного движения за счет обмена информацией между транспортными средствами (OBU, от англ. board unit) и объектами дорожной инфраструктуры (RSU, от англ. road-side unit). OBU могут работать в режиме V2V (от англ. Vehicular to Vehicular), V2I (от англ. Vehicular to Infrastructure) или в гибридном режиме, что позволяет за одну или несколько итераций обмениваться сообщениями со всеми участниками сети. Это обеспечивает информирование и предупреждение водителей транспортных средств о возможных препятствиях (ремонтных работах, ограничении скорости и т.п.), а также возможность организации согласованных действий (смена полос, приоритетный проезд перекрестков и т.п.). Поэтому любое нарушение функционирования VANET автоматически влияет на безопасность людей и техники на дороге, что возводит вопросы угроз ее информационной безопасности в ранг «сверхактуальных», о чем свидетельствует нарастающее количество публикаций на эту тему. Последнее требует научного осмысления, и первым шагом в этом направлении является классификация угроз.

В отсутствии единой устоявшейся классификации рассмотрим подходы и классификационные признаки, которые авторы применяют в своих тематических обзорах за последние 5 лет.

Так, например, авторы [1] предполагают классифицировать угрозы на следующие группы:

a) MonitoringAttack. По мнению авторов, данная угроза позволяет прослушивать сеть и выявлять в ней не только перемещения транспортных средств, но и прослушивать переговоры между транспортными средствами полиции (силовых ведомств), выявлять в них интересующую информацию и передавать заинтересованными лицам для уклонения от ответственности;

b) SocialAttack (психологическая атака на человека). Авторы представляют автомобильную сеть как некий чат, в котором абоненты могут обмениваться сообщениями, и отправив широковещательное «freak»-сообщение, спровоцировать водителей к нарушению ПДД;

c) TimingAttack– атака на сеть с целью увеличения задержки маршрутизации сообщений путем их физического «удерживания» на транспортном средстве злоумышленника;

d) ApplicationAttack– атаки на мобильное приложение с целью получитьвозможность изменять отправляемые в сеть сообщения;

[1] Исследование выполнено при финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (Соглашение № 14.604.21.0165, уникальный идентификатор проекта RFMEFI60417X0165).

e) NetworkAttack– атаки на оборудование сети (например, DoS, Sybil, NodeImpersonation).

Данная классификация с незначительными вариациями встречается и в другой работе [2].

В основу этих классификаций (в попытке учесть специфику автомобильных беспроводных сетей) положен признак объекта атаки (трафик, водитель, сетевая топология, мобильное приложение, сетевое оборудование); однако эти объекты принадлежат разным сущностным категориям.

Другие авторы [3] предлагают классифицировать угрозы как атаки на доступность (attacks on availability), конфиденциальность (attacks on confidentiality), целостность и достоверность (attacks on integrity and data trust), неотказуемость (attacks on non-repudiation/ accountability), аутентификацию и идентификацию (attacks on authenticity and identification).

Здесь в качестве классификационного признака нетрудно заметить «три с половиной кита» информационной безопасности (свойства конфиденциальности, целостности и доступности информации, а также неотказуемость факта ее обладания/передачи – дань международным стандартам [4]), однако к ним «прилагаются» также атаки на механизмы защиты (аутентификацию и идентификацию), что с неизбежностью приводит к нарушению основного принципа классификации.

Авторы [5] предлагают разделить угрозы на активные и пассивные, а последние – в соответствии с моделью взаимодействия открытых систем по уровням, выделяя следующие: физический (например, Jamming), сетевой (Sybil), транспортный (Man in the Middle), прикладной (Repudiation), – и, по всей видимости, отдельная группа содержит атаки, воздействующие на несколько уровней (DDoS). В этом варианте, хотя классификационные признаки и системны («пассивный» vs «активный» – категориальные пары, а уровни взаимодействия – конечны и стандартизованы), однако угрозы классифицируются без учета специфики автомобильных беспроводных сетей (т.е. характерны для любой телекоммуникационной сети).

Анализ публикаций, посвященных классификации угроз информационной безопасности VANET показал, что они либо используют некорректные классификационные признаки, либо не учитывают специфику автомобильных беспроводных сетей. Причина такого положения, на наш взгляд, кроется в недостаточной академичности современных «писателей» на тему информационной безопасности ввиду их увлеченности «best practice» в ущерб теоретической и методологической подготовке. По этой же причине серьезной проблемой для систематизации (и последующей удачной классификации) также является наблюдаемая терминологическая путаница, приводящая к смещению и смешению понятий «уязвимость», «источник угрозы», «ущерб», «атака» и собственно «угроза». С другой стороны, классификация угроз информационной безопасности VANET является нетривиальной задачей даже для «классических ученых» ввиду ее сложности, как объекта изучения, так как это не просто специфический сегмент беспроводной сети, а набор разнородных устройств от транспондера до автомобиля и светофора; и каждая из угроз здесь должна быть рассмотрена с позиции возможности ее реализации по отношению к конкретному слою: OBU, RSU, V2V, V2I. В этом контексте более прагматичная (т.е. ориентированная на прогнозирование и генерацию требований по информационной безопасности) классификация может быть получена при использовании в качестве классификационного признака главных элементов интеллектуальной транспортной системы: транспортных средств, транспортной инфраструктуры и интерфейса информационно-технического взаимодействия, – как объектов атаки.

СПИСОКЛИТЕРАТУРЫ

1. Sumra I.A., Ahmad I., Hasbullah H., Manan J. Classes of attacks in VANET // Proceedings of the Saudi International Electronics, Communications and Photonics Conference (SIECPC), Riyadh, Saudi Arabia, 2011, pp. 1-5.
2. Sumra I.A., Hasbullah H.B., Manan J, Ahmad I., Alghazzawi D.M. Classification of Attacks in Vehicular Ad hoc Network (VANET) // Information, 2013, vol. 16, no. 5, pp. 2995-3004.
3. Hasrouny H., Samhat A.E., Bassil C., Laouiti A. VANet Security Challenges and Solutions: A Survey // Vehicular Communications, 2017, vol. 7, pp. 7-20.
4. ISO/IEC 13335-1:2004 Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management. ISO, 2004.
5. Nema M., Stalin S., Lokhande V. Analysis of Attacks and Challenges in VANET // International Journal of Emerging Technology and Advanced Engineering, 2014, vol. 4, iss. 7, pp. 831-835.

УДК 004.056, 0004.75

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ КОНВЕРГЕНТНЫХ ТЕХНОЛОГИЙ В ОБЛАЧНОЙ СРЕДЕ

Воробьев Владимир Иванович, Левоневский Дмитрий Константинович,
Рыжков Сергей Романович, Фаткиева Роза Равильевна
Санкт-Петербургский институт информатики и автоматизации РАН
Россия, Санкт-Петербург, 14 линия, 39
e-mail: Ryzhkov@iias.spb.su

Аннотация. В статье рассматриваются проблемы ногомерности периметра вычислительных систем, соотнесения цифрового и географического ландшафтов, районирования и обработки событий информационной безопасности облачной инфраструктуры с применением нейросети как механизма контроля миграции данных. Предложен нейросетевой метод распознавания факта пересечения

границы с учётом совместного влияния многих статистических параметров и способов отслеживания и локации информации на основе геотегирования. Проанализированы основные риски для облачных инфраструктур с точки зрения атак, приведены методики повышения системной безопасности на основе использования геометок.

Ключевые слова: *облака, облачные вычисления, периметр безопасности, геотегирование, нейронные сети, управление информационной безопасностью.*

SECURITY MANAGEMENT OF CONVERGENT TECHNOLOGIES IN THE CLOUDY ENVIRONMENT

Vorobiev Vladimir, Levonevskii Dmitrii, Ryzhkov Sergei, Fatkieva Roza
St. Petersburg Institute for Informatics and Automation of Russian Academy of Science
Russia, St. Petersburg, 14-ya liniya V. O., 39
e-mail: Ryzhkov@iias.spb.su

Abstract. Neural networks as a tool for developing a method for information security perimeter management described below. Digital mapping and geographic landscape, zoning. Neural network for recognition of the fact of border crossing taking into the joint effect of thousands of statistical parameters, analysis of tracking and location information on the basis of the main risks for cloud infrastructures showed in terms of attacks and methods of improving system security through the use of geotagging. Event handling information security cloud infrastructure, using neural networks as a mechanism of control over migration of the data.Presented the review of the various approaches to classification of attacks on cloud infrastructure from a position of use of geolocation technology to create a cloud computing perimeter.An overview of the taxonomies of the attacks on cloud infrastructure. An overview of subject tracking technologies for guaranteed attribution. The possibility of applying the technology of geotagging as a tool of territorial control of the data movement throughout their life cycle.

Keywords: *cloud computing, security perimeter, geotagging.*

Введение. Для виртуализации и развертывания облачных сред в конвергентной инфраструктуре характерны проблемы урегулирования конкурирующих приоритетов виртуализации сред и обеспечения существующих требований к безопасности и визуальному контролю[1]. Конвергентная инфраструктура в мире ИТ подразумевает объединение вычислительных ресурсов по принципу уменьшения числа элементов в системе и упрощения задач управления инфраструктурой, что весьма актуально ввиду постоянного роста объемов, обрабатываемых данных и повышения требовательности приложений. Конвергенция ресурсов физических сер еров в виртуальный сервер требует перестройки работы межсетевого экрана, систем обнаружения вторжений и других средств защиты. Физические системы безопасности не контролируют трафик междузонами виртуальных машин в облачной среде, так как они исключены из процесса маршрутизации передачи данных. Динамическая организация виртуальных машин делает проблему безопасности рабочих нагрузок в ЦОД еще более острой.

С другой стороны, узлы фильтрации, ограничивающие доступ физическим и юридическим лицам к веб-ресурсам по закону № 139 ФЗ, требуют сбора данных с фильтрующих устройств, т.е. проблема контроля периметра (границы зоны легитимного доступа сети), кроме обеспечения безопасности пользователя, носит и правовой характер.

Традиционные средства фильтрации расположены по периметру локальной сети, демилитаризованной зоны (ДМЗ), либо по периметру сети провайдера. Однако имеется статистика, показывающая, что примерно 25% пользователей выходят за периметр стационарных сетей[1]. Мотивы нарушения периметра различны и возможно противоречивы. Попробуем представить, что происходит в динамически изменяемой виртуальной сети. Одним из путей выхода за периметр является маршрут доступа к ЦОД, где контроль периметра осуществляется в стационарных точках. В таблице 1 приводятся результаты анализа средств фильтрации [1].

Таблица 1

Анализ средств фильтрации

	Застава-IDS	SkyDNSZapret ISP	Carbon	Периметр-Ф	СКАТ
Возможность загрузки реестра с сайта РКН по ЭП	+	+	+	+	+
Возможность дополнения списков региональными блокировками	+	+	+	-	+
Схема реализации решения на оборудовании провайдера	+	+	+	+	+
Доп. услуги по фильтрации отдельных клиентов и интеграция с биллингами, белые списки	+	+	+	-	+
Схема мониторинга	+	-	+	-	+

В [1] предлагается один из возможных путей контроля периметра на пути доступа к ЦОД для фильтрации по реестру запрещенных сайтов:

- сбор и анализ статистики по протоколам и направлениям;
- разметка приоритета трафика в зависимости от протокола;
- распределение канала доступа между абонентами с уведомлениями;
- защита от DoS и DDoS-атак;
- Lawfulinterception — перехват трафика;
- запись http-запросов;
- предфильтр- Система оперативно-розыскных мероприятий(СОРМ).

Данный метод не включает географического контроля периметра, предусматривающего задание географического расположения легитимной облачной зоны и регистрация выходов за её границы.

В отличие от [1], в [2] предлагается географический контроль маршрута продвижения трафика пользователя, что позволяет преодолеть ряд трудностей (вмешательство в настройки пунктов фильтрации, совместимость используемых средств защиты, и т.д.). В данной статье рассматривается задача определения сетевого периметра в зависимости от варианта задачи контроля выхода за периметр. Географическое определение периметра с помощью геометок, рассмотренное в [2], позволяет определить один из возможных контуров периметра. Если учитывать географическое размещение пунктов фильтрации, получим другой контур. Для облачной структуры с учетом разворачивания виртуальной машины получим третий вариант периметра. Далее нам предстоит сравнить все варианты с допустимым расположением периметра.

Периметр стационарной сети – это граница между находящейся в собственности, локально управляемой стороной сети и общественной, обычно управляемой провайдером. В качестве сетевого периметра традиционно выступает физическая и логическая подсеть, предоставляющая внешний доступ к ресурсам собственника, фактически периметр является неотделимой частью защищаемой сети, что представлено на рис. 1.

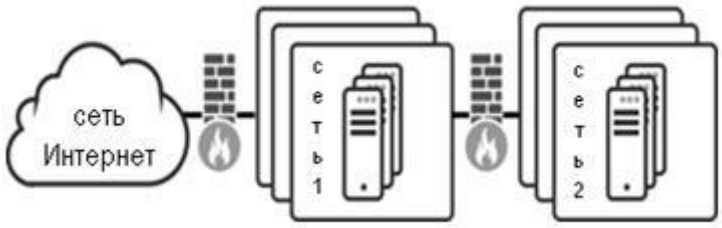


Рис. 1. Классическая схема, где внешний доступ предоставляется логической подсети.

Физическая сеть представляет собой границу внутри, которой расположено оборудование сети. Подсеть представляет собой границу логического сегмента, который сам является самостоятельной разделяемой средой с меньшим количеством узлов.

Периметр в облачных вычислениях виртуализован, т.к. он определяется параметрами виртуальной среды и выполняемых приложений. В этом случае периметр динамически изменяется, размывается за счёт многоуровневой туннелированной вложенности. Каждый уровень вложенности позволяет создать снимок своего периметра, что в свою очередь позволяет, используя привязку к физическому периметру, затем разместить их на карте. Облачные вычисления позволяют отказаться от классической архитектуры, где в случае нарушения периметра вся защищаемая сеть находится под угрозой. Периметр безопасности в облаке, поставляемый как услуга, физически и логически отделяет зону защищаемой подсети, как отображено на рис. 2.

Рис. 2. Периметр безопасности в облаке

Физический периметр в системах контроля и управления доступом (СКУД), также оперирует понятием «граница», в контексте границы контролируемой зоны. Таким образом, осуществляется районирование географического расположения электронно-вычислительной распределенной структуры с целью обнаружения пересечения границ выделенного района, занимаемого подсетью, и

оценки угроз обрабатываемым данным [4, 5, 6]. Необходимость постановки этой проблемы обусловлена следующими причинами:

– Обеспечение правового гарантированного доступа к отечественным и зарубежным информационным ресурсам, что оказывает прямое влияние на возможность реализации конституционных прав граждан на доступ к информации и на обеспечение национальной безопасности России [7].

– Обеспечение безопасности миграции и объединения данных и приложений при использовании конвергентных структур в географически распределенных облачных хранилищах [8, 9].

– Использование гетерогенных вычислительных средств, составляющих основу облачных вычислений, зачастую разнородных и от разных производителей, что может повлечь за собой не только сбои в работе виртуальной среды, но и множество различных атак на неё [10, 11].

– Повышение вероятности преодоления систем защиты при получении несанкционированного доступа к управлению виртуальной средой [12, 13].

– Ограничение доступа физическим и юридическим лицам к сайтам в Интернете, содержащим информацию, распространение которой в Российской Федерации запрещено.

– Необходимость атрибуции отслеживания перемещения информации с целью создания матрицы доступа и контроля уровня предоставляемых прав [14-16].

Перечисленные причины имеют одно общее свойство – географическое местоположение (узлов, ресурсов, пользователей) как контролируемый фактор.

Дэвид Кларк отмечал, что виртуальное пространство обладает свойством многомерности (соответственно- много границ), т.е., киберпространство не однородно и имеет несколько уровней. В частности, им предложена модель, в которой существует четыре уровня киберпространства [19]:

1. Физический уровень содержит все аппаратные устройства. Физическая инфраструктура географически расположена в "реальном пространстве", и, таким образом, является предметом различных юрисдикций.

2. Логический уровень, который включает в себя программное обеспечение, алгоритмы и протоколы.

3. Уровень мета-контента, который описывает всю информацию в киберпространстве.

4. Социальный уровень, состоящий из всех индивидов, использующих и формирующих характер киберпространства.

По сути, социальный слой включает правительства, частный сектор, социум и субъекты технического сообщества.

Важным условием для обеспечения информационной безопасности информационной системы, построенной с использованием технологий облачных вычислений, является определение потенциального места проведения атаки с целью её предотвращения. Одним из способов определения адреса атаки являются геолокационные метки (геометки [18]).

Геометки созданные на основе криптографически заверенного эталонного состояния, предоставляют инструмент контроля перемещения «частной собственности» (данных и программ) в виртуальной среде путем сопоставления их географического положения с разрешенным периметром. Учитывая значение геополитики в глобальной сети Интернет, становятся востребованы инструменты контроля перемещения данных, с использованием понятий «геолокация» и «геоограждение».

Традиционные промышленные системы безопасности класса SIEM (Securityinformationandeventmanagement), системы управления информацией и событиями в системе безопасности типа IBM QRadar SIEM уступают системам предотвращения, обнаружения и проверки типа CiscoCognitiveThreatAnalytics.Последняя описывается в [21] как призванная задержать и отвлечь атакующих от выполнения своих целей из-за быстрорастущих методов автоматизации атак.

На рынке программно-аппаратных средств обеспечения представлен широкий набор средств безопасности, но недостаточно внимания уделяется тому, как этот набор инструментов может быть использован. Все это приводит к необходимости разработки методов определения географического положения периметров, миграции данных и заданий с достаточной точностью. В работе используется нейросетевой метод, основанный на многоальтернативном дискретном накоплении [2].

Предлагается использовать систему классификации географических объектов на базе метода многоальтернативного дискретного накопления и надежного автоматического различения объектов на географической карте. Классификация — процесс сортировки (распределения по классам) элементов изображения (пикселов) на конечное число классов на основе значений их атрибутов. Сравнение методов классификации, показывает, что нет «лучшего» алгоритма классификации. Каждый алгоритм обладает определенным набором своих характеристик, и нужно подбирать наиболее подходящий алгоритм под конкретные задачи. Мы выбрали нейронные сети, учитывая, что точность классификации выше у этого метода. А для обучения нейронных можно использовать результаты контролируемой классификации.

Предлагается использовать метод многоальтернативного дискретного накопления [3]. Метод сводится к наложению эталонных символов на анализируемый символ и к последующему подсчету

суммы произведений совпадающих значений яркости и вынесению решения о символе по большинству суммы произведений. Предварительно подбиралось такое значение виртуальной яркости (заменяющей яркость черного цвета при двух градационном изображении) при котором достигалось безошибочное различение объектов-эталонов — оптимизация на обучающей выборке. Можно показать, что такой алгоритм эквивалентен подсчету количества совпадающих яркостей черного цвета при наложении эталонных символов на текущий символ и вынесению решения о номере объекта-эталона по большинству совпадений.

Используется 7 изображений (каналов): RED + GREEN + BLUE «серый» канал, каналы RED, GREEN, BLUE, а также полусуммы изображений RED + GREEN, RED + BLUE, GREEN + BLUE. Все 7 каналов рассматриваются как один вектор.

Для каждого пиксела изображения определяется множество пикселов, попадающих в зрачок анализирующей системы с центром в этом пикселе, яркости и координаты яркостей этого множества. Затем последовательно накладываются все эталоны на отобранное множество, и для каждого эталона подсчитывается число голосов в его пользу. После подсчета всех голосов выбирается решение в пользу того класса, для которого количество голосов максимально. Соответствующее решение выводится, а анализируемый пиксел подсвечивается условным цветом. Если при этом получается нулевая сумма, то этот вариант считается отказом от классификации и подсвечивается яркостью белого цвета. Алгоритм формирования изображения решения после первого голосования можно представить схемой искусственного неадаптивного нейрона рис. 3.

Здесь T — количество пикселей изображения, Xk — множество пикселей, попадающих в зрачок системы с центром в k-той точке, YI— множество пикселей, соответствующих i-му эталону, ∑ — суммирование количества совпадений яркостей пикселей в множествах Xk и Yi, MAXi — выбор в качестве решения для k-той точки изображения того эталона и соответствующего ему класса для которого количество совпадений яркостей пикселов в множествах Xk и Yi максимально.

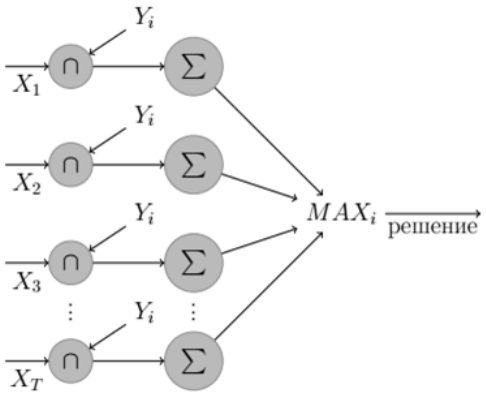


Рис.3. Структура искусственного неадаптивного нейрона

Для более быстрой классификации изображений необходимы большие вычислительные ресурсы параллельная обработка данных.

Рассматриваемый алгоритм классификации не имеет ветвей решения или частей алгоритма, которые могут выполняться параллельно. Очевидным решением в этом случае будет распараллеливание по данным.

Задача классификации разделена на две части, как на рис. 4.

Управляющая часть — процесс, существующий в единственном экземпляре. Отвечает за считывание изображений, параметров классификации, разбиение изображения на части, распределение задач, синхронизацию, склеивание и запись изображений. Именно эта часть будет отвечать за сложную логику, «знать» о разных форматах изображений, способах кодирования цвета, количестве процессов классификации и т.д.

Классифицирующая часть — процессы, занимающие оставшиеся процессоры, максимально облегчены, отвечают за получение снимка и параметров, классификацию.

Основным способом взаимодействия параллельных процессов является передача сообщений друг другу с помощью технологии MPI – MessagePassingInterface.

Оценим производительность параллельного алгоритма классификации на размере карты, близком к реальным задачам. Накладные расходы на пересылку карт, формирование частей и обратную склейку минимальны.

В таблице 2 приведены результаты временных затрат на классификацию и определен оптимальный размер карты для классификации одним процессом.

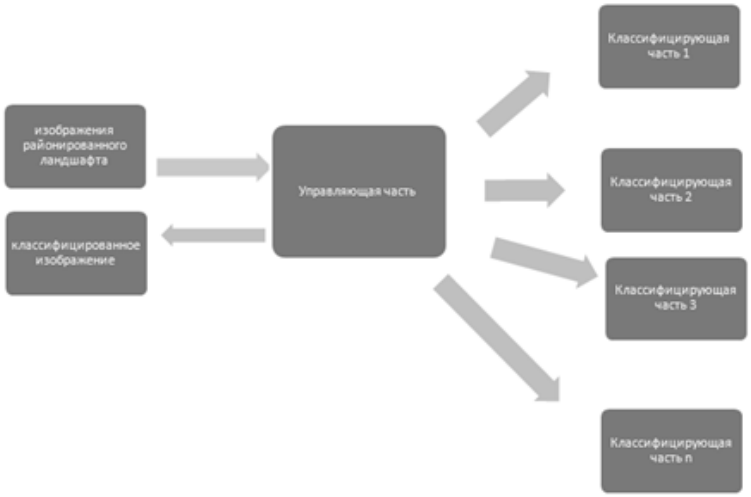


Рис. 4. Архитектура параллельного алгоритма

Таблица 2

Результаты временных затрат на классификацию

Кол-во процессов	Максимальное время классификации одним процессом, с	Суммарное время, с	Размер части,
2	102.32	217.70	17.846
3	48.32	136.56	8.921
5	27.34	101.98	4.460
10	12.26	80.84	1.982
15	8.04	75.63	1.273
20	7.36	74.07	0.937
25	4.85	71.93	0.743
30	8.73	76.06	0.612

Измерение производительности параллельной реализации алгоритма, размер карты 4609 на 3872 пикселей

Заключение. Картографирование и распознавание зон легитимного доступа в облачной структуре становится важной задачей в целях обеспечения безопасности ЦОД, включающей регистрацию, визуализацию и предупреждение о нарушениях в конвергентных структурах. Предложенный метод неинвазивный и не нарушает настроек и работоспособности программных средств. Комплексное решение проблем контроля доступа позволяет обеспечить решение нормативно-правовых задач. Работа выполнена по программе президиума РАН 1.П5.

СПИСОК ЛИТЕРАТУРЫ

1. Блог компании ИТ-ГРАДURL: https://habrahabr.ru/company/it-grad/
2. Воробьев В. И., Рыжков С. Р., Фаткиева Р. Р.Применение нейронных сетей для управления периметром информационной безопасности. 9-я конференция«Информационные технологии в управлении»(ИТУ-2016).
3. Vorobiev V.I., Evnevich E.L., Levonevskiy D.K. Classifying large aerospace images by themulti-alternative discrete accumulation method, The 13th International Symposium on Neural Networks (ISNN 2016), St. Petersburg, July 6-8, 2016.
4. Морель Д. А., Зубкова К. В. К вопросу о средствах репрезентации рефлексивного концепта" Периметр безопасности": сопоставительный аспект исследования //Альманах современной науки и образования: межвуз. сб. науч. тр. – 2008. – №. 3. – С. 101-105.
5. Жуков А. В. О числе π //М.: МЦМНО. – 2002.
6. Беккер М. Я. и др. Информационная безопасность при облачных вычислениях: проблемы и перспективы //Научно-технический вестник информационных технологий, механики и оптики. – 2011. – №. 1. – С. 71.
7. Гюнтер Е. С., Нарутта Н. Н., Шахов В. Г. «ОБЛАЧНЫЕ» ВЫЧИСЛЕНИЯ И ПРОБЛЕМЫ ИХ БЕЗОПАСНОСТИ //Омский научный вестник. – 2013. – №. 2-120.
8. Саклаков В. М. Облачные вычисления: современные модели предоставления услуг и возможные риски //Молодежь и современные информационные технологии: сборник трудов XIII Международной научно-практической конференции студентов, аспирантов и молодых ученых, г. Томск, 9-13 ноября 2015 г. Т. 2. -Томск, 2016. – Изд-во ТПУ, 2016. – Т. 2. – С. 104-106.
9. Фролов Д. Б., Грунюшкина С. А. Старостин АВ Информационная геополитика и сеть Интернет //М.: РФК-Имидж Лаб. – 2008.

10. Р. М. Юсупов, В.М. Шишкин, “О некоторых противоречиях в решении проблембинформационной безопасности”, Тр. СПИИРАН, 6 (2008), 11–23
11. Петров Д. Л. Оптимальный алгоритм миграции данных в масштабируемых облачных хранилищах //Управление большими системами: сборник трудов. – 2010. – №. 30.
12. Amoroso E. G. Fundamentals of Computer Security Technology. Prentice Hall PTR, Upper Saddle River, NJ. 1994.
13. Коваленко О. С. ОБЗОР СОСТОЯНИЙ, ПРОБЛЕМ И ПЕРСПЕКТИВ ХРАНЕНИЯ И АНАЛИЗА ДАННЫХ В «ОБЛАКЕ».
14. Каменщиков А. А. Облачные технологии и интероперабельность информационных систем в здравоохранении //Журнал радиоэлектроники. – 2013. – №. 2.
15. Чемеркин В. В. Облачные вычисления как инструмент обработки конфиденциальной информации //Вестник Российского государственного гуманитарного университета. – 2012. – №. 14 (94).
16. Mauw S., Verschuren J. H. S., de Vink E. P. A formalization of anonymity and onion routing //Computer Security–ESORICS 2004. – Springer Berlin Heidelberg, 2004. – С. 109-124.
17. Shao X., Li L. Data-driven multi-touch attribution models //Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining. – ACM, 2011. – С. 258-264.
18. White R. W. et al. From devices to people: Attribution of search activity in multi-user settings //Proceedings of the 23rd international conference on World wide web. – ACM, 2014. – С. 431-442.
19. David Clark, Characterizing cyberspace: past, present and future, MIT/CSAIL Working Paper, 12 March 2010. http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf
20. Boyns M. R. et al. Method and apparatus for aggregating and presenting data associated with geographic locations :заяв. пат. 12/470,475 США. – 2009.
21. Kinsner W. Towards cognitive security systems //Cognitive Informatics & Cognitive Computing (ICCI* CC), 2012 IEEE 11th International Conference on. – IEEE, 2012. – С. 539–539.
22. Цыбаков Б.С., Яковлев В.П. О точности восстановления функций с помощью конечного числа членов ряда Котельникова. Радиотехника и электроника, 1959, т. 4, № 3, с. 234

УДК 006.056

КВАЛИМЕТРИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Воробьев Владимир Иванович[1], Фаткиева Роза Равильевна[2]
[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Россия, Санкт-Петербург, ул. Профессора Попова, 5
[2] Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова,
Россия, Санкт-Петербург, 1-я Красноармейская ул., 1,
e-mails: vvi@iias.spb.su

Аннотация. В докладе рассмотрены процессы классификации, определения градаций и интервальных оценок и арифметизации качественных характеристик объектов различной природы с помощью введения измерительных шкал. Показана необходимость анализа защищенности в зависимости от типа информации.

Ключевые слова: *моделирование; информационная безопасность; квалиметрическая шкала; классификация; неопределенность выбора.*

QUALIMETRY OF INFORMATION ASSET SECURITY

Vorobiev Vladimir[1],FatkievaRoza[2]
[1]St. Petersburg State Electrotechnical University "LETI"
Russia, St. Petersburg, st. Professor Popov, 5
[2]Baltic State Technical University "VOENMEKh" them. D.F. Ustinov
Russia, St. Petersburg, 1-st Red Army str., 1
e-mail: vvi@iias.spb.su

Abstract. This paper considers processes of classifying, determining grades and interval evaluations, and arithmetization of qualitative characteristics of various objects by means of applying measuring scales. Necessity of security analysis depending on the information type is shown.

Keywords: *modeling; information security; qualimetric scale; classification; uncertainty of making decisions.*

Формирование базовых информационных ресурсов (БИР) опирается на разработку методов и математических моделей упорядочения, классификации, оценку объектов различной природы, включая качественные характеристики: достоверность данных, ценность данных, сведения о правах доступа и т.д. Задача классификации, определения градаций и интервальных оценок и арифметизация качественных характеристик можно решать с помощью введения измерительных шкал. Все данные, входящие в состав БИР, должны подвергаться анализу на защищенность. В частности, даже персональные данные как паспортные, адрес, фамилия и т.д. могут иметь различные вариации в зависимости от источника. Защищенность можно оценивать с помощью квалиметрической шкалы. Например, если данные из закрытых источников, то отсчет на шкале будет иметь значение 1, если источники незащищены, то значение 0. Промежуточные значения в зависимости от совпадения могут принимать значения от 0 до 1.

Задача классификации имеет также черты неопределенности выбора, связанные с наличием разных систем классификации, существующих в разных ведомствах. Наша задача состоит в сведении всех шкал в единую шкалу.Множество исходных характеристик X = {x1, …, xn}, на котором задана структура отношений S, описывающая взаимодействие соответствующих градаций. Реляционная структура M = (X;S) является обобщенной измерительной шкалой. Примером таких «нечисловых» характеристик являются оценки уровня защиты данных. Структуры подобных шкал можно описать в первом приближении, используя отношение порядка S>, определяемого на множестве X как подмножество декартова произведения. В работе[1] доказано, что произвольная шкала измерения редуцируется к совокупности линейных ординальных шкал.

СПИСОК ЛИТЕРАТУРЫ

1. Хованов Н.В. Анализ и синтез показателей при информационном дефиците. –СПб.: Издательство Санкт-Петербургского университета 1996. –196 с.
2. Г.Г. Малинецкий, С.П. Курдюмов Синергетика и прогноз. //Новое в синергетике. – М.: Наука, 2002. –478 с.

УДК 004.56

МЕТОДЫ ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ ЗАДАЧИ ПОИСКА УЯЗВИМОСТЕЙ В ИСПОЛНЯЕМЫХ ФАЙЛАХ

Демидов Роман Алексеевич
Санкт-Петербургский политехнический университетПетра Великого
Россия, Санкт-Петербург, ул. Политехническая, 29
e-mail: rd@ibks.spbstu.ru

Аннотация. В работе рассмотрен подход к поиску уязвимостей в исполняемом коде на основе глубокого обучения. Строится алгоритм, который классифицирует образцы кода по наличию уязвимостей определенных классов. На вспомогательных подзадачах с большим объемом тренировочных данных строятся векторные представления для инструкций и вызовов внешнего API. Графы передачи управления входных программ предварительно приводятся к унифицированному представлению фиксированного размера. Многослойная свёрточная нейронная сеть принимает на вход унифицированные представления графов программ и обучается на помеченных данных об уязвимостях. Обученная сеть классифицирует новые образцы кода на наличие уязвимостей.

Ключевые слова: *поиск уязвимостей; глубокое обучение; граф передачи управления; свёрточная сеть; векторные представления.*

DEEP LEARNING METHODS FOR VULNERABILITY SEARCH IN EXECUTABLE CODE

Demidov Roman
St. Petersburg State Polytechnical University
Russia, St. Petersburg, Politechnicheskya str., 29
e-mail: rd@ibks.spbstu.ru

Abstract. The paper describes a deep learning approach of vulnerability research in executablecode. The algorithm is constructed for code samples classification based on existence of certain classes of vulnerabilities. With huge auxiliary dataset of cheap labeled data, we construct vector representations for machine instructions and API calls. Control flow graphs of input programs are mapping to the fixed size unified representation. That code representations form the inputs of multilayer convolutional network that being trained on the well-labeledexpensive data of vulnerability existence. Well trained network used to classify new code samples.

Keywords: *vulnerability search; deep learning; control flow graph; convolutional neural network; vector representations.*

Предлагается новый взгляд на проблему поиска уязвимостей. Если код рассматривать как один из дискретных видов данных наравне с текстами или изображениями, то наличие уязвимости – это одно из абстрактных свойств таких данных, которое не описывается напрямую в терминах инструкций кода и их параметров. В рамках подхода из бинарного кода обучается иерархия абстрактных свойств, приводящих к уязвимостям различных классов.

Для корректного обучения классификатора необходимо соблюдение следующих условий:

– Похожие по действию инструкции должны иметь похожие представления. Машинный код инструкции/её индекс в словаре не удовлетворяют этому свойству.

– Графовая структура кода и вытекающие из неё свойства (достижимость вершин, соседство инструкций до и после команд передачи управления и т.д.) должны быть учтены и закодированы для дальнейшего использования этой информации при обучении.

Построение разрешающего алгоритма, который обучается классифицировать код по наличию в нем уязвимостей, происходит поэтапно:

1. Сначала строятся векторные представления инструкций исходя из их семантического смысла. Для инкапсуляции семантики инструкций в вещественных векторах фиксированного размера используется обучение с переносом. Вспомогательная сеть обучается сравнивать семантический смысл участков кода друг с другом. В процессе обучения отдельные инструкции кода неявно отображаются в векторное пространство высокой размерности таким образом, что близкие по семантике инструкции имеют близкие образы [1]. Данные для обучения на этом этапе генерируются автоматически с помощью сравнения состояния памяти после эмуляции участков кода. Обученные векторные представления инструкций далее используются в качестве их нового описания.

2. Входные программы, ввиду наличия команд передачи управления, представляются в графовом виде. Для дальнейшей обработки с помощью свёрточной нейронной сети строится единое нормализованное представление входных графов программ. Вершины нумеруются так, чтобы похожие по окружению. Выбираются опорные вершины (векторные представления отдельных инструкций), которые будут описывать различные варианты локальных связей между соседними инструкциями в графах передачи управления. Для каждой выбранной вершины определяются нормализованные списки ее соседей (с дополнением до единого размера). Таким образом, различные варианты соседства в графе передачи управления формируют различные ядра свёртки, используемые далее в первом слое свёрточной сети для формирования карт признаков.

3. Многослойная свёрточная нейронная сеть [] в качестве входа первого слоя принимает ранее нормализованные графовые представления программ (п. 2). Для вычисления выходного сигнала сети послойно строятся карты признаков с ядрами свёртки различных конфигураций (п. 2). Выходной слой сети содержит вероятности принадлежности входного примера к одному из классов уязвимостей. Для обучения сети на помеченных образцах кода используется алгоритм обратного распространения ошибки. Имея для каждого тренировочного примера эталонный выходной сигнал (класс уязвимости в данном образце кода), весовые коэффициенты нейронной сети подстраиваются с целью наилучшего соответствия выхода сети эталонному сигналу.

Априорные сильные ограничения, выраженные в локальности ядер свёртки, препятствуют переобучению сети. Вместо этого сеть учится выделять существенные факторы, наличие которых в коде приводят к уязвимостям различных классов. При поступлении на вход новых образцов кода сеть использует ранее обученный каскад последовательных преобразований для выдачи выходного распределения образца по классам уязвимостей.

Предлагаемый подход позволяет построить классификатор исполняемого кода по классам уязвимостей. Для успешного обучения необходимо наличие тренировочного набора образцов кода с пометками о наличии уязвимостей.

СПИСОК ЛИТЕРАТУРЫ

1. Daniel Jurafsky & James H. Martin. Semantics with Dense Vectors. Speech and Language Processing, 2017
2. Yoon Kim, Convolutional Neural Networks for Sentence Classification, Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing, p. 1746–1751, 2014

УДК 004.056

МОДЕЛИРОВАНИЕ И АНАЛИЗ ЗАЩИЩЕННОСТИ КОММУНИКАЦИОННОЙ СЕТИ УПРАВЛЕНИЯ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ НА БАЗЕ УСТРОЙСТВ XBEE

Десницкий Василий Алексеевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mail: desnitsky@comsec.spb.ru

Аннотация. Предметом исследования является беспроводная мобильная самоорганизующаяся коммуникационная сеть поддержки и оперативного управления в чрезвычайных ситуациях. Автономный характер узлов сети, меняющиеся во времени сетевая топология и пропускная способность каналов связи, а также динамическая маршрутизация в сети обуславливает необходимость повышенных требований к защищенности таких систем. В работе проводится моделирование коммуникационной сети на базе беспроводных устройств XBee и анализ ее защищенности с учетом возможных инцидентов информационной безопасности.

Ключевые слова: *коммуникационная самоорганизующаяся сеть; моделирование; анализ защищенности; XBee.*

MODELING AND SECURITY ANALYSIS OF A COMMUNICATION NETWORK FOR CRISIS MANAGAMENT ON THE BASE OF XBEE DEVICES

Desnitsky Vasily
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
e-mail: desnitsky@comsec.spb.ru

Abstract. The subject of the study is a wireless mobile self-organizing mesh communication network for crisis management in emergency situations. The autonomous nature of the network nodes, network topology and bandwidth of communication channels changing runtime as well as the dynamic routing in the network determine a necessity of increased security requirements to such systems. A communication network on the base of XBee wireless devices is modeled and its security is analyzed in terms of possible information security incidents.

Keywords: *communication mesh network; modeling; security analysis; XBee.*

Работа направлена на решение задач обеспечения согласованности совместной работы встроенных устройств оперативных служб для решения задач реагирования и управления в чрезвычайных ситуациях.

Разработана модель предметной области мобильных распределенной коммуникационной сети поддержки и оперативного управления в чрезвычайных ситуациях, которая обеспечивает совместную и согласованную работу различных служб, задействованных устройств, сенсоров, актуаторов и связующего коммуникационного и вычислительного оборудования.

Система представляет мобильный командный программно-аппаратный комплекс для поддержки коммуникационных сервисов в рамках оперативного управления и реагирования в чрезвычайных ситуациях. К коммуникационным сервисам относятся передача видео и аудио данных, текстовых сообщений, изображений, сервисы доступа к базам данным, веб-сервисы и др.

Система основывается на базе устройств Digi XBee серии 2, позволяющих построить самоорганизующуюся беспроводную сеть с топологией, изменяющейся динамически в зависимости от географического положения узлов, интенсивности трафика, конфигурационных настроек перехода устройств в режим сна и обратно, других характеристик.

В общем случае узлы сети могут представлять собой, как персональные портативные устройства с заданным набором сенсоров и актуаторов, так и встраиваться в технические объекты инфраструктуры управляющего штаба, наземные транспортные средства, дроны с различными характеристиками энергопотребления, автономности, вычислительными и коммуникационными мощностями.

Отметим, что сети устройств XBee имеют следующие ограничения. Допустимый размер одной XBee-сети - не более чем нескольких сот устройств. При более чем 300 устройств существенно возрастает служебный трафик и, соответственно, падает пропускная способность, в т.ч. за счет разрешения возникающих конфликтов при случайном распределении адресов, увеличения времени обнаружения устройств и прокладки маршрутов, ограничения ОЗУ для хранения больших таблиц маршрутизации. Поэтому при необходимости большего числа взаимосвязанных коммуникационных моделей сеть делят на несколько подсетей – кластеров, каждая из которых управляется своим координатором с решением вопросов маршрутизации сообщений между узлами разных подсетей. Помимо этого, максимально разумное число ретрансляций пакета в сети ZigBee не должно превышать 10–30 хопов.

Также отметим, что модули XBee не ориентированы на использование в системах быстро движущихся объектах, однако моделирование таких систем с использованием модулей XBee при определенных ограничениях возможно.

Устройства XBee имеют некоторые ограниченные встроенные средства обеспечения информационной безопасности, которые могут отличаться в зависимости от модификаций устройства и версии его прошивки. В частности, актуальная в настоящий момент прошивка XB24-ZB из средств защиты предоставляет только средства симметричного шифрования на основе алгоритма AES с ключом 128 бит. При этом при помощи данного крипто примитива осуществляется шифрование только полезной назгрузки, тогда как структура пакета, в том числе идентификаторы PAN ID и MAC оказывается незащищенной перед потенциальным нарушителем. Также в рамках текущей версии модулей XBee не решается задача автоматического распределения/смены ключей, которые осуществляются вручную в режиме настройки параметров прошивки устройства. Поэтому дополнительная защита сети на основе устройств XBee должна реализовываться на прикладном уровне взаимодействия.

По типу доступа и уровню возможностей выделяется пять категорий возможных нарушителей информационной безопасности целевой системы [1, 2].

Нарушитель типа 0 способен осуществлять лишь атаки социальной инженерии, воздействуя вербально или при помощи легитимных каналов связи на персонал системы или третьих лиц. Приемы социальной инженерии могут использоваться также и нарушителями других типов в качестве предваряющих действий атаки с целью получения сведений о системе, паролей, RFID-карт и пр.

Нарушитель типа 1 может совершать атаки, на потоки данных, передаваемых через внешний TCP/IP-интерфейс глобального координатора сети [3]. Это могут быть MITM-атаки на уровне пакетов, универсальные сетевые атаки (DoS-атаки); атаки на базе уязвимостей сетевых драйверов, крипто анализ сообщений, атаки на системы аутентификации, обновления и др.

Нарушитель типа 2 расширяет данный перечень атак воздействиями на беспроводные интерфейсы мобильной сети – прослушиванием, анализом, модификацией и подделкой беспроводного трафика, исходящего или входящего на некоторый интерфейс – XBee-интерфейсы узлов сети, Wi-Fi-интерфейс координатора сети и пр. Нарушитель типа 2 может также осуществлять атаку по сторонним каналам на получение информации, а также атаку на снижение или нарушение доступности беспроводного канала путем внесения электромагнитных шумов (jamming-атака).

Нарушитель типа 3 имеет доступ к проводным интерфейсам, модулям ввода/вывода устройства (сенсорам), доступ нарушителя к которым не предполагает необходимость вскрытия корпуса устройства. Ввиду отсутствия у терминальных устройств, используемых при работе мобильной сети портов проводной коммуникации, нарушитель типа 3 может осуществлять атаку несанкционированного использования устройством после обхода процедуры аутентификации в случае физического захвата устройства.

В случае невозможности обхода процедуры аутентификации нарушитель типа 3 может оказать физические воздействия на сенсор терминального устройства, в результате чего в сеть будут отправляться некорректные показания. Помимо этого, нарушитель типа 3 может совершить атаку экранирования, для снижения стабильности и пропускной способности канала связи через данный узел, увеличив энергопотребление устройства или нарушив связность сети, а также осуществить атаку по отключению устройства от автономного источника питания [4].

Для нарушителя типа 4 мобильная сеть представляется как множество взаимосвязанных микросхем, коммуникационных интерфейсов, сенсоров, к которым атакующий имеет неограниченный доступ. Нарушитель может проводить считывание информации с пинов и дизассемблировать программный код. В частности, нарушитель типа 4 может осуществить атаку подмены контроллера на некотором терминальном устройстве с сохранением соответствующего модуля XBee, получив тем самым управляемое извне устройство, которое может использоваться легальным пользователем системы в дальнейших мероприятиях управления и реагирования в чрезвычайных ситуациях.

Работа выполнена при финансовой поддержке РФФИ (проекты 15-07-07451, 16-29-09482 офи_м) и бюджетных тем № 0073-2015-0004.

СПИСОК ЛИТЕРАТУРЫ

1. Abraham, D.G., Dolan, G.M., Double, G.P., Stevens, J.V. Transaction security system. // IBM Systems Journal. 1991. V. 30(2). P.206–228.
2. Rae, A.J., Wildman, L.P.: A Taxonomy of Attacks on Secure Devices. // Australian Information Warfare and IT Security. 2030. P. 251-264.
3. Chechulin A., Kotenko I., Desnitsky V. An approach for network information flow analysis for systems of embedded components. // Lecture Notes In Computer Science. Springer-Verlag GmbH. 2012. V. 7531. P. 146-155.
4. Desnitsky V., Kotenko I. Expert knowledge based design and verification of secure systems with embedded devices. // Lecture Notes In Computer Science. Springer-Verlag GmbH. 2014. V. 8708. P. 194-210.

УДК 004.056

МОДЕЛИ, МЕТОДИКА И АЛГОРИТМЫ ВЫБОРА ЗАЩИТНЫХ МЕР НА ОСНОВЕ СИСТЕМЫ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ ДЛЯ ПРОАКТИВНОГО И РЕАКТИВНОГО ПРОТИВОДЕЙСТВИЯ АТАКАМ В КОМПЬЮТЕРНЫХ СЕТЯХ

Дойникова Елена Владимировна[1,2], Котенко Игорь Витальевич[1,2]
[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
[2] Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: doynikova@comsec.spb.ru, ivkote@comsec.spb.ru

Аннотация. В работе рассматривается проблема противодействия атакам в компьютерных сетях. Определена методика и алгоритмы, позволяющие реализовать проактивный и реактивный выбор защитных мер. Введены аналитические модели для оценки защищенности и выбора защитных мер и связи между ними. Разработана система показателей защищенности и ее применение в рамках предложенной методики. Описаны и обоснованы требования к соответствующим моделям, методике и алгоритмам, а также их особенности, обусловленные поставленными требованиями.

Ключевые слова: *защита информации; аналитические модели; противодействие атакам; защитные меры; показатели защищенности.*

MODELS, TECHNIQUE AND ALGORITHMS OF THE COUNTERMEASURE SELECTION BASED ON THE SYSTEM OF SECURITY METRICS FOR THE PROACTIVE AND REACTIVE RESPONSE TO ATTACKS IN COMPUTER NETWORKS

Doynikova Elena[1,2],Kotenko Igor[1,2]
[1]St. Petersburg Institute for Informatics and Automation of RussianAcademy of Sciences
Russia, St. Petersburg, 14 Liniya, 39

[2] St. Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), Russia,St. Petersburg, Kronverkskiy pr.,49
e-mails: doynikova@comsec.spb.ru, ivkote@comsec.spb.ru

Abstract. The paper considers the problem of response to attacks in the computer networks. It specifies the technique and algorithms that implement proactive and reactive countermeasure selection. It also introduces analytical models for the security assessment and countermeasure selection and relations between them. The paper describes the developed system of security metrics and its application in scope of the developed technique. Finally, the paper provides and substantiates requirements to the appropriate models, technique and algorithms, and their features caused by these requirements.

Keywords: *information security; response to attacks; analytical models; countermeasures; security metrics.*

В настоящее время ввиду объемов и сложности компьютерных сетей, применяемых повсеместно, одной из актуальных задач является противодействие атакам в компьютерных сетях на основе комплексного автоматизированного управления информационной безопасностью [1].

Комплексное управление информационной безопасностью подразумевает выполнение ряда процессов, к которым в том числе относятся [2]: идентификация рисков, анализ и оценка рисков, определение и оценка различных вариантов обработки риска. Для их эффективного выполнения были предложены различные стандарты, инструменты, модели и методики. Тем не менее, задача комплексного своевременного автоматизированного противодействия атакам в компьютерных сетях на основе адекватных количественных показателей защищенности на текущий момент остается нерешенной.

В данной работе для решения поставленной задачи был разработан комплекс взаимосвязанных моделей, методик и алгоритмов. При их разработке принимались во внимание следующие требования: комплексный учет множества данных, предоставляемых различными средствами мониторинга и оценки защищенности компьютерных сетей; выбор защитных мер на основе адекватных количественных показателей; возможность получения результата в любой момент времени; автоматизация процесса вычисления показателей и выбора защитных мер; учет стоимостных характеристик при определении выигрыша в случае реализации защитных мер; выбор наиболее адекватных защитных мер на основе доступных входных данных; проактивный и реактивный выбор защитных мер.

При этом предполагается, что выполнение требований комплексного учета множества данных и выбора защитных мер на основе адекватных количественных показателей позволит выбирать эффективные защитные меры. Для удовлетворения этих требований в рамках проведенного исследования был разработан комплекс взаимосвязанных моделей, показателей защищенности и алгоритмов их вычисления для выбора защитных мер. Модели были сформированы и связаны в соответствии с основными компонентами информационной безопасности и отношениями между ними. К ним относятся модель компьютерной сети, модель зависимостей сервисов, модель атак, модель атакующего, модель событий, модель контрмер. По этому же принципу были выделены основные уровни показателей защищенности: топологический – показатели данного уровня вычисляются на основе модели сети; атак – показатели данного уровня вычисляются на основе модели атак; атакующего – показатели данного уровня вычисляются на основе модели атакующего; событий – показатели данного уровня вычисляются на основе модели событий; контрмер – показатели данного уровня вычисляются на основе модели контрмеры; и интегральный – показатели данного уровня вычисляются на основе показателей предыдущих уровней.

Выполнение требований возможности получения результата в любой момент времени, автоматизации процесса вычисления показателей и выбора защитных мер, и выбора наиболее адекватных защитных мер на основе доступных входных данных позволит своевременно выбирать и реализовывать защитные меры на любом этапе функционирования системы. Возможность получения результата в любой момент времени достигается за счет многоуровневого характера методики выбора защитных мер. Выделяются статический и динамический уровни работы методики. При этом статический уровень, в свою очередь, делится на топологический уровень, уровень атак и атакующего (аналогично уровням выделения показателей защищенности). Динамический уровень методики соответствует уровню событий системы показателей защищенности. Уровни связаны между собой иерархически от нижнего топологического уровня к уровню атак, уровню атакующего и верхнему уровню событий. В процессе работы методики алгоритмы разных уровней запускаются в параллельных потоках в зависимости от наличия данных (моделей и показателей) соответствующих уровней. При поступлении команды на вывод результата (то есть набора выбранных контрмер), выводится результат верхнего из тех уровней, процесс выбора контрмер для которых завершен. Алгоритмы разных уровней носят рекурсивный характер относительно объектов воздействия защитных мер (на топологическом уровне объекты воздействия – это подсеть, хост, программное и аппаратное обеспечение, уязвимости, на остальных уровнях – подграф, узел графа, уязвимости). В

процессе работы алгоритмов вначале выбираются контрмеры с наибольшей областью воздействия. Затем, в случае необходимости, выбираются контрмеры с меньшей областью воздействия. Работа алгоритмов завершается, когда контрмерами охвачены все объекты с неприемлемым уровнем риска, или если рассмотрены все возможные варианты контрмер. Для выбора контрмер введен интегральный показатель, рассчитываемый на основе множества показателей разных уровней таким образом, чтобы максимизировать выигрыш от реализации контрмер, и минимизировать затраты на их реализацию. Автоматизация процесса вычисления показателей и выбора защитных мер достигается, в том числе, за счет применения открытых стандартов для представления и обработки данных, и использования данных, предоставляемых различными средствами мониторинга защищенности и данных из открытых баз уязвимостей, программно-аппаратного обеспечения, конфигураций, слабых мест и других.

Выполнение требований учета стоимостных характеристик при определении выигрыша в случае реализации защитных мер и выбора защитных мер на основе адекватных количественных показателей позволит связать цели организации в целом с целями управления информационной безопасностью, а также количественно обосновать необходимость реализации защитных мер. Для удовлетворения этих требований вводится модель зависимостей сервисов в виде графа. Данная модель позволяет определить стоимость всех информационно-технологических активов организации на основе стоимости основных бизнес-активов организации. Это позволяет при выборе контрмер учесть потери от успешной реализации атакующих действий. Кроме того, при выборе контрмер учитывается стоимость реализации контрмер.

Введение требования проактивного и реактивного выбора защитных мер связано с тем, что невозможно полностью исключить риск успешной реализации атак на компьютерную сеть на этапе проектирования системы. Тем не менее, на основе результатов моделирования возможных атак и оценки защищенности, можно определить набор средств защиты, которые позволят на этапе эксплуатации системы реализовать защитные меры против обнаруженных атак. Для моделирования возможных атак используется байесовский граф атак. Такая модель с одной стороны позволяет проактивно определить риски успешного выполнения атак, а с другой стороны, пересчитать их в случае возникновения инцидентов безопасности и использовать полученные результаты для реактивного выбора контрмер.

Работа выполняется при поддержке РФФИ (проекты 15-07-07451, 16-37-00338, 16-29-09482 офи_м) и при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007 в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И.В., Саенко И.Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. № 3 (22). СПб.: Наука, 2012. С.84-100.
2. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. — Введ. 2006–12–27. — М.: Стандартинформ, 2008. — 26 с.

УДК 004.652

МОДЕЛЬ ЗАЩИЩЕННОГО ХРАНЕНИЯ БОЛЬШИХ СЛАБОСТРУКТУРИРОВАННЫХ ДАННЫХ

Евневич Елена Людвиговна, Петров Михаил Юрьевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14 линия В.О., 39
e-mails: eva@iias.spb.su, miha@iias.spb.su

Аннотация. Рассмотрены вопросы ассоциативного хранения слабоструктурированных данных. Предложена онтологическая модель метаописания данных.

Ключевые слова: *метаданные; онтологии; когнитивные системы.*

SEMI-STRUCTURED BIG DATA PROTECTED STORAGE MODEL

Evnevich Elena[1], Petrov Mikhail[2]
[1,2]St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 line, 39
e-mails: eva@iias.spb.su, miha@iias.spb.su

Abstract. Consideration is given to the issues of semi-structured data storage. Ontologic model of meta data description is proposed.

Keywords: *meta data; ontologies; cognitive systems.*

В настоящее время подавляющее большинство предметных областей оперируют с использованием методов больших данных. Количество таких предметных областей и объёмы данных неуклонно возрастают, что делает обработку больших данных не только актуальным, но и весьма перспективным направлением исследований. Значительную часть обрабатываемых больших данных

составляют слабоструктурированные данные, требующие создания новых интерфейсов, в частности когнитивных.

Для эффективной обработки больших данных одного когнитивного интерфейса недостаточно. В настоящее время частично реализуется когнитивная система обработки и хранения данных, потому что имеющиеся доступные средства (Hadoop) громоздки, требуют больших объемов памяти и вычислительных ресурсов и соответственно дорогостоящи. Концепция когнитивного хранения, предложенная IBM, позволяет создать гибкую и динамичную систему, способную более эффективно хранить данные за счет дифференцирования самых важных данных и менее востребованных, что экономит место на носителях. Помимо определения частоты использования данных и их нагрузочных характеристик, показатель ценности данных также можно использовать для определения уровней предоставляемого сервиса и требований к безопасности.

Подобно системе хранения задача обработки данных требует также новых методов реализации на основе когнитивных принципов. В качестве примера можно привести операционную систему для распространения облачных вычислений и Интернета Вещей Heaven and Earth (небо и земля). Система комбинирует операционную систему искусственного интеллекта (AIS) с операционной системой естественного интеллекта (NIS) через информационный интерфейс между реальным физическим пространством и электронным виртуальным пространством в графическом методе, который выстраивает цепочку значений (ценностей), а затем комбинирует когнитивную систему с CAD RS/ICT в полностью новую операционную систему. Облачная система преобразуется в систему небо-земля, которая концентрируется на цепочке ценностей. Естественный интеллект и искусственный интеллект объединяются и интегрируются как основные линии процесса апгрейда общей интеллектуальной интегрированной системы (IIS).

Разработку системы обработки и хранения данных можно производить с использованием онтологического анализа. Преимущества онтологического анализа состоят в гибкости онтологии, т.е. возможности быстрого изменения, в том числе добавления новых элементов данных без кардинальной переработки уже созданной онтологии. Кроме того, онтологический анализ данных позволяет разделить их на некоторые классы, что, в свою очередь, даёт возможность разработки процедур обработки данных, принадлежащих к одному классу. Каждой процедуре приписывается одно из возможных «состояний». Совокупность всех сведений, с которыми пользователь работает в настоящее время или работал ранее, выделяются в отдельную сущность, рассматриваемую как информационные ресурсы, например, файлы, заметки, посещенные веб- страницы, письма и пр. В рамках предлагаемого подхода в качестве информационных ресурсов рассматриваются RDF - ресурсы. Структура информационного ресурса описывается с помощью OWL - онтологии пользователя, которую при необходимости пользователь может изменять, добавляя новые классы и свойства, а также расширяя уже имеющиеся.

Онтологический анализ запроса пользователя начинается с составления метаданных, часть из которых сопровождают контент: тип запрашиваемого документа и его содержание, предметные области, к которым документ имеет отношение, ключевые слова (теги). Другая часть метаданных составляется на основе данных, полученных в результате семантического анализа содержания документа, который дает возможность выявить часто используемые термины, ключевые слова, используемые для установления похожести документа на другие документы и установления соответствия требованиям пользователей. В процессе онтологического моделирования понятия разделяются на категории: выделение в общие категории ресурсов, находящихся в разделах иерархической структуры, организованной пользователем и выделение в общие категории на основании добавленных пользователем метаданных. Структурирование метаданных позволяет осуществить обработку атрибутов, а также сформировать группы пользователей как по атрибутам, так и по интересам.

Заключение.

Предложенная онтологическая модель защищенного хранения данных позволяет разрабатывать эффективные и сравнительно не ресурсоемкие способы хранения и защиты данных.

СПИСОК ЛИТЕРАТУРЫ

1. Дэррил Тафт. IBM представляет когнитивное хранение данных. https://www.itweek.ru/infrastructure/article/detail.php?ID=184568
2. Воробьев В.И., Евневич Е.Л. Онтологические методы контроля доступа в облачной среде. Информационная безопасность социально-экономических систем: монография /Апатова Н.В. и др./ Под ред. д.т.н. профессора О.В. Бойченко. – Симферополь: ИП Зуева Т.В., 2017, 348 с.
3. Воробьев В.И., Монахова Т.В. Метамодель защиты метаданных. Информационная безопасность социально-экономических систем: монография /Апатова Н.В. и др./ Под ред. д.т.н. профессора О.В. Бойченко. – Симферополь: ИП Зуева Т.В., 2017, 348 с.

УДК: 004.78

ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ «УМНЫЙ ГОРОД»

Жигадло Валентин Эдуардович
Филиал ФГУП ЦНИИС – ЛО ЦНИИС
194223, Россия, Санкт-Петербург, ул. Варшавская, 11
e-mail: zve@mail.ru

Аннотация. В современных условиях эффективность процесса управления жизнедеятельностью современных крупных городов и регионов определяется наличием и качеством используемых информационных систем управления. В докладе подробно рассматриваются особенности построения системы управления городским хозяйством, основанной на принципах «Умного Города».

Ключевые слова: *безопасный город; умный город; управление транспортом; информационная система.*

PRINCIPLES OF CREATION OF THE «SMARTCITY» SYSTEM

Zhigadlo Valentin
Federal State Unitary Enterprise TSNIIS branch – LO TSNIIS
194223, Russia, St. Petersburg, Varshavskaya str., 11
e-mail: zve@mail.ru

Abstract. In modern conditions efficiency of process of management of activity of the modern large cities and regions is defined by existence and quality of the used information management systems. In the report features of creation of the control system of municipal economy based on the principles of "Smart City" in detail are considered.

Keywords: *safe city; "Smart City"; management of transport; information system.*

В мировой практике, в целом, под «Smart Sity» понимают реализацию комплекса решений по следующим направлениям: решения, ориентированные на «зеленые» технологии, основным посылом которых является снижение выбросов CO2 и использование возобновляемых источников электроэнергии; решения, обеспечивающие транспортную безопасность и эффективное управление транспортными потоками; решения, обеспечивающие охрану правопорядка и безопасность жизнедеятельности населения; решения, направленные на накопление и перераспределение энергии; решения, направленные на раздельный сбор и переработку ТБО; системы городского информирования.

Предлагаемые и реализуемые за рубежом и в России стратегии, концепции, подходы, модели и проекты по созданию Умных городов, можно свести к общей модели, включающей семь составляющих: умная экономика; энергоэффективность и ресурсосбережение; умная среда обитания; мобильность; умное население; умное управление; комфортность проживания.

«Умный Город» для городских властей – это: обеспечение мер безопасности и эффективное управление деятельностью экстренных и оперативных служб; мониторинг и управление угрозами и чрезвычайными ситуациями, влияющими на среду обитания; переработка и утилизация отходов производства и потребления (мусора), раздельный сбор мусора; очистка сточных вод, управление ливневыми стоками; энергоэффективность и ресурсосбережение (использование энергосберегающих, экологичных и безопасных технологий и решений в топливно-энергетическом комплексе (включая водоснабжение), ЖКХ, градостроительстве и на транспорте); комфортное жильё, умный дом/здание; система городского оперативного оповещения; многофункциональные центры (МФЦ), обслуживающие жителей и организации по принципу «одного окна», государственные и муниципальные услуги, а также дополнительные информационные, заказывающие и платежные сервисы в электронном виде в сфере ЖКХ, связи, транспорта, торговли, быта, банковского обслуживания, налогов, страхования, культуры, спорта, отдыха, туризма и пр; городское видеонаблюдение для предотвращения правонарушений; система фиксации нарушений ПДД и сбора штрафов; планирование расходов на оплату коммунальных услуг бюджетных организаций; удобный общественный транспорт, транспортная доступность, снижение загруженности УДС, отслеживание «пробок» и управление дорожным движением; градостроительство и землепользование в соответствии с принципами архитектуры нового урбанизма и промышленной архитектуры индустриальных парков и их совместимости; экологический и биологический мониторинг окружающей среды (атмосфера, гидросфера, почва, биосфера), использование возобновляемых источников энергии (солнечные, ветряные, геотермальные, приливные, биотопливные); GPS/GLONASS мониторинг городского транспорта и транспорта экстренных служб; обслуживание общегородской инфраструктуры; прозрачное предоставление образовательных услуг (электронное образование); прозрачное предоставление медицинских услуг (электронная и телемедицина); информационно-картографическое обеспечение и т.п.

«Умный Город» для жителей - это: система самообслуживания через личный кабинет для оплаты услуг ЖКХ, электронная запись для получения бытовых или медицинских услуг; решения по экономному расходованию всех видов коммунальных ресурсов; быстрое предоставление государственных услуг городскими властями; карта жителя города (ID, проезд в городском транспорте, система предоставления скидок, оплата за товары и услуги); внутридомовое (входы в здания, лифты, этажные площадки...) и наружное видеонаблюдение, системы видеоконференцсвязи (ВКС) и телеприсутствия; интеллектуальная транспортная система, парковочный информатор, электронное расписание (графики работы и обслуживания, транспорт); системы погодно-климатического и экологического мониторинга; градостроительство и землепользование в соответствии с принципами архитектуры нового урбанизма (пешеходная доступность в частности); скоростная ИКТ-инфраструктура (проводная и беспроводная), публичные и социальные сервисы на базе открытых интернет-порталов (Web-приложений) и мобильных приложений; высокотехнологичные многофункциональные персональные ИКТ-устройства, мобильные, информационные и платежные сервисы, электронные пластиковые карты (ID, различные виды платежей, безопасность, банковские, транспортные и др. виды услуг).

«Умный Город» для управляющих и ресурсо-снабжающих компаний - это: система автоматизированного сбора данных с приборов учета и мониторинга оборудования инженерных систем, находящихся на обслуживании; система автоматизированного управления инженерными системами, находящимися на обслуживании, погодно-ориентированное поведение инженерных систем; своевременное выставление счетов и контроль оплат, планирование расходов на оплату коммунальных услуг бюджетных организаций; решения по экономному расходованию всех видов коммунальных ресурсов; отчеты в режиме реального времени по потреблению всех видов ресурсов, как в масштабе города, так и в более мелкой детализации (квартал, здание, квартира, организация и т.п.); краткосрочные и долгосрочные прогнозы по потреблению ресурсов; видео-мониторинг за подотчётной территорией; обеспечение автоматического и диспетчерского отключения систем при наступлении природных или техногенных катастроф.

СПИСОК ЛИТЕРАТУРЫ

1. Резолюция 4-й конференции «Система распределенных ситуационных центров − 2014», 16−17 октября, г. Воронеж.
2. Резолюция 5-й конференции «Система распределенных ситуационных центров», 7-9 октября 2015 г., г. Ярославль.
3. Концепция построения и развития аппаратно-программного комплекса «Безопасный город», утвержденная распоряжением Правительства Российской Федерации №2446-р от 03 декабря 2014 года;
4. Наставление по организации деятельности центров управления в кризисных ситуациях МЧС России, Москва, 2012 г.
5. В. Чернышев. Инфраструктура «Умного Города» - оптимальные решения, CNews Conferences, Москва, 2013 г.

УДК 004.75

ОЦЕНКА ЭФФЕКТИВНОСТИ ПЛАТФОРМЫ РАСПРЕДЕЛЕННОГО АНАЛИЗА ДАННЫХ HADOOP В СРАВНЕНИИ С ПЛАТФОРМОЙ SPARK ДЛЯ ЦЕЛЕЙ СЕТЕВОЙ БЕЗОПАСНОСТИ

Кушнеревич Алексей Геннадьевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mail: kushnerervich@comsec.spb.ru

Аннотация. В материале раскрывается одна из проблем систем мониторинга и управления безопасностью сети. Рассмотрен вариант решения проблемы через использованиеплатформ распределенной обработки данных Hadoopи Spark. Проведено описание особенностей и свойств платформ, также проведено сравнение производительности на частной задаче.

Ключевые слова: *распределенная обработка; защита информации; большие данные; Hadoop; Spark.*

EVALUATION OF THE EFFICIENCY OF HADOOP DISTRIBUTED DATA ANALYSIS PLATFORM IN COMPARISON WITH SPARK PLATFORM FOR NETWORK SECURITY GOALS

Kushnerevich Alexey
St. Petersburg Institute for Informatics and Automation of RussianAcademy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
e-mail: kushnerervich@comsec.spb.ru

Abstract. The article considers one of problems of network security monitoring and management. The variant of the solution of the problem through the use of distributed data processing platforms Hadoop and Spark is considered. The features and properties of the platforms have been described, and a performance comparison has been performed on a particular task.

Keywords: *distributed processing; information security; big data; Hadoop; Spark.*

Современные сети генерируют большие объемы данных, которые необходимо обрабатывать в целях обеспечения безопасности. Возможности вертикального масштабирования вычислительных ресурсов ограничены и в больших сетях системы мониторинга и управления безопасностью могут несправляться с поставленной задачей.

Для того, чтобы удовлетворить потребностям по производительности в больших сетях необходимо разрабатывать системы мониторинга и управления безопасностью, основанные на принципе горизонтального масштабирования вычислительных ресурсов [1]. Когда увеличение производительности достигается не за счет установки более мощных комплектующих, а за счет включения в вычислительную сеть параллельных машин, работающих сообща над поставленными задачами.

К наиболее популярным системам консолидации вычислительных ресурсов множества машин относят такие платформы распределенной и параллельной обработки данных как Hadoop и Spark. Предлагается организовывать системы мониторинга и управления безопасностью в больших сетях поверх подобных платформ распределенной обработки данных.

В дальнейшем, чтобы снизить расходы на закупки оборудования требуется выявить наиболее эффективную платформу распределенной обработки для того или иного случая.

Платформы распределенной обработки Hadoop и Spark хотя и имеют общее название, обладают рядом существенных отличий и, соответственно, различными требованиями к аппаратному обеспечению.

Hadoop использует модель распределенной обработки MapReduce. В этой модели начальная задача разбивается на однотипные более мелкие, которые могут быть вычислены параллельно или распределенно.

Такая операция называется Map (отображение). Вторая операция – Reduce, предназначена для того, чтобы после получения независимых друг от друга результатов операции Map выполнять действия над ними. Стоит отметить, что операция Reduce так же выполняется распредленно, поэтому она должна удовлетворять свойству кумулятивности. Reduce принимает результаты Map попарно, где первым операндом является результат предыдущей итерации Reduce, а вторым очередной результат операции Map.

Spark применяет модель RDD-блоков (распределенных наборов). На вход поступают локальные коллекции данных, которые переводятся в независимые распределенные коллекции данных RDD. Над независимыми данными проводятся однотипные преобразования, далее результаты переводятся из распределенных коллекция обратно в локальные. Особенностью Spark является то, что все операции над данными делятся на так называемые трансформации и действия. К операциям трансформации относят только те операции, которые не подразумевают материализацию результата. К операциям действия напротив относятся только операции действия. Например, такие как collect(), count(), которые дают непосредственную команду к выводу результата на экран или к сохранению его на диск в виде файла.

В нашем случае мы сравнивали две системы в рамках задачи нахождения событий безопасности «сканирование портов».

Событие безопасности «сканирование портов» регистрируется в том случае, если с одного и того же IP-адреса на другой IP-адрес были высланы пакеты на более чем 10 портов, причем на каждый порт пришлось менее 5 пакетов.

Испытания проводились на записи трафика объемом 1,5 ГБ. На платформе виртуализации ESXi было создано 7 виртуальных машин под управлением Ubuntu Server. Сервер, на котором был установлен ESXi, имеет в распоряжении 2x6-ядерных процессора E5-2620v2 @ 2.1 GHz, мат. плата X9DRL-3F. Были подготовлены конфигурации кластера из 3-х, 5-ти, 7-ми машин для тестирования.

Конфигурации виртуальных машин:

– 2-поточный 2.0 GHz CPU;
– 4 ГБ ОЗУ.

Результаты представлены в таблице 1.

Таблица 1

К-во машин в кластере	Время обработки, сек	
	Hadoop	Spark
3	328,18	42,58
5	276,35	21,64
7	258,93	18,01

Как можно видеть из таблицы Spark на порядок опережает Hadoop по производительности на такой задаче. Такая разница объясняется тем, что Spark кэширует все вычисления в оперативной памяти, в том время как Hadoop записывает данные на диск после каждой итерации Map, Reduce. Тем не менее, существуют задачи, для которых из-за большого объема данных кэширование

невозможно или ограничено количеством оперативной памяти. С увеличением объемов обрабатываемых данных преимущество Spark будет нивелироваться.

Работа выполняется при поддержке РФФИ (проекты 15-07-07451, 16-37-00338, 16-29-09482 офи_м) и при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007 в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И.В., Саенко И.Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. № 3 (22). СПб.: Наука, 2012. С.84-100.

УДК 004

АНАЛИЗ МЕТОДОВ ОБНАРУЖЕНИЯ МНОГОУРОВНЕВЫХ СТЕГАНОВСТАВОК В BMP-ИЗОБРАЖЕНИЯХ

Минаева Тамара Александровна, Волошина Наталия Викторовна, Беззатеев Сергей Валентинович
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: minaeva-toma-ya@yandex.ru, nataliv@yandex.ru, bsv@aanet.ru

Аннотация. В статье рассматриваются методы стеганоанализа для выявления стегановставок в BMP-изображениях, скрытых путем замены наименее значимых битпри условии многоуровневого встраивания. Исследуется уровень шума, создаваемый таким встраиванием, и проводится анализ влияния уровня встраивания, с целью поиска наиболее пригодных для встраивания стегановставки путем простой замены битов изображения битами встраиваемого сообщения при условии визуальной незаметности вносимых искажений. Значительное внимание уделяется исследованию и анализу двух наиболее эффективных методов стеганоанализа: регулярно-сингулярному методу (RS-методу) и методу Хи-квадрат.

Ключевые слова: *стеганография; цифровые водяные знаки; скрытый канал; стеганоанализ; многоуровневое встраивание.*

ANALYSIS OF STEGANOANALYTICAL METHODS FOR MULTYLEVELEMBEDDING IN BMP-IMAGES

Minaeva Tamara, Voloshina Natalia, Bezzateev Sergey
St. Petersburg National Research University of Information Technologies, Mechanics and Optics “ITMO”
Russia, St. Petersburg, Kronverksky Prospect 49
e-mails: minaeva-toma-ya@yandex.ru, nataliv@yandex.ru, bsv@aanet.ru

Abstract. The article dedicated to the methods of steganoanalysis methods for detection of embedding in BMP-images that are hidden by replacing the multilevel least significant bits. The noise level that is created by such embedding is investigated. The analysis of embedding level is performed to define the most suitable bits for multilevel embedding taking into account its invisibility. The research and analysis of the two most effective methods of steganoanalysis such as regular-singular method (RS-method) and Chi-square method was performed.

Keyword: *steganography; digital watermarking, hidden channel; steganoanalysis; multilevel embedding.*

Введение. Поскольку на сегодняшний день Интернет, используемый в качестве среды для обмена данными, является открытым источником, то проблемы безопасности, такие как модификация и перехват данных, становятся все более актуальными. Были разработаны несколько подходов для безопасного обмена данными в Интернете. Криптография является одним из таких методов. Суть этого метода в том, что секретная информация преобразуется в неузнаваемую форму, таким образом, что только пользователь, у которого есть секретный ключ, может преобразовать ее обратно в исходную информацию [1]. Но в некоторых ситуациях мало превратить секретную информацию в неузнаваемую форму, необходимо полностью сокрыть факт передачи секретной информации по каналу связи, чем и занимается стеганография.

Стеганография — наука о методах сокрытия секретных данных внутри других не сокрытых данных с использованием алгоритмов внедрения. Одним из способов организации скрытого канала связи является внедрение информационных сообщений в цифровые объекты, свободно распространяемые по сети. В качестве таких объектов выступают цифровые изображения, аудио- и видеофайлы и т.д. [1, 3].

Одновременно с появлением стеганографических методов встраивания секретной информации появились методы стеганоанализа, позволяющие выявить скрываемую информацию в цифровых объектах (контейнерах) [2, 4, 6].

На сегодняшний день одним из самых распространенных стеганографических методов сокрытия информации в изображениях является метод замены наименее значимых бит (НЗБ или

LSB). Идея метода заключается в замене наименее значимого бита, например,в байтах цветового представления точек изображения, битом скрываемого сообщения.

Такой метод может применяться к растровым изображениям, не прошедшим компрессию с частотным преобразованием, например, изображения формата BMP [2, 4, 5].

В статье будет рассмотрен универсальный метод Хи-квадрат, использующий анализ статистических характеристик и разработанный в 2000 году А. Пфитцманом и А. Вестфелдом [2]. А также, будет рассмотрен направленный статистический метод, впервые опубликованный в 2001 г. коллективом ученых под руководством Дж. Фридрих – RS-метод [2].

Анализ уровня шума. Для исследования эффективности работы стеганоаналитических методов в BMP-изображение встраивалась, путем замены наименее значимых бит, биты псевдослучайной последовательности различной длины. Использование псевдослучайных сообщений в качестве тестовых объясняется тем, что для сокрытия содержания сообщения оно может быть предварительно зашифровано.

Перед тем как будут рассмотрены статистические методы, оценим уровень шума, создаваемый встраиванием в НЗБ BMP-изображения. Для того чтобы найти уровень искажения изображения (PSNR) необходимо вычислить абсолютную оценку - среднеквадратичное отклонение реального сигнала, описывающего изображение, от полезного:

$$RMSE = \sqrt{\frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} | I(i,j) - K(i,j) |^2}{mn}}, \quad (1)$$

где RMSE – среднеквадратичное отклонение исходного сигнала, описывающего изображение, от измененного; I(i,j) – значение элемента заполненного контейнера; K(i,j) - значение элемента «пустого» контейнера; m×n– количество элементов в контейнере.

Используя среднеквадратичное отклонение может быть вычислена относительная оценка – пиковое отношение полезного сигнала к шуму PSNR, измеряемое в децибелах:

$$PSNR = 20\log_{10}\left(\frac{A_{\max}}{RMSE}\right), \quad (2)$$

где PSNR – пиковое отношение полезного сигнала к шуму; A_{max} - максимальное значение сигнала (максимальное значение, принимаемое пикселем изображения, для полноцветного BMP-изображения A_{max} = 255); RMSE – среднеквадратичное отклонение реального сигнала, описывающего изображение, от полезного.

Сообщение может встраиваться в контейнер не только путем замены только первого наименее значимого бита, но и более старших. На основании статей [7-9] можно утверждать, что встраивать скрываемое сообщение можно от одного до четырех младших бит значений. При изменении значений бит в старших битовых плоскостях происходит, как видно на рисунке 1, сильное искажение изображения.

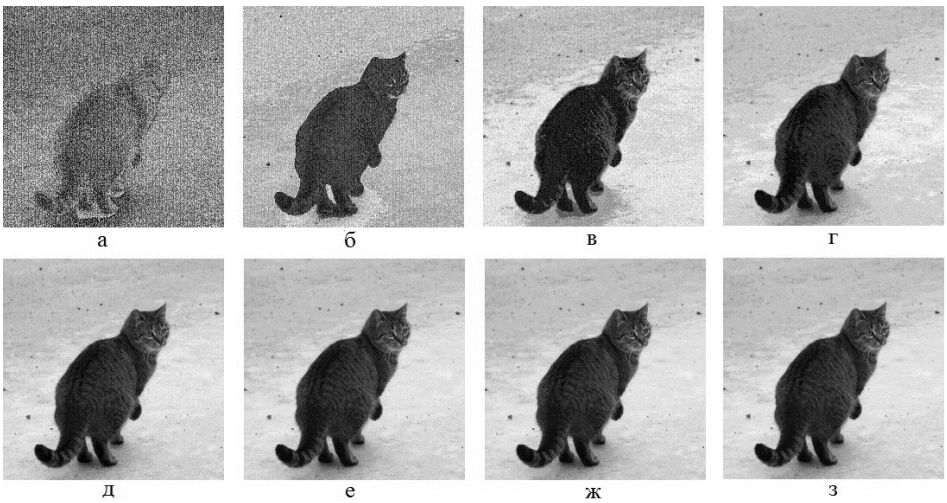


Рис. 1. BMP-изображения со встроенным сообщением в разных битах значений цветовых составляющих пикселей (а – встроено в 8 бит; б – встроено в 7 бит; в – встроено в 6 бит; г – встроено в 5 бит; д – встроено в 4 бит; е – встроено в 3 бит; ж – встроено во 2 бит; з – встроено в 1 бит)

Результат встраивания в BMP-изображения визуально не заметен при встраивании сообщения в последние четыре бита (рисунок 1).

В таблице 1 произведен сравнительный анализ BMP-изображений со встроенным сообщением в различные биты значений цветовых составляющих пикселей на основе таких параметров как PSNR иRMSE. Известно, что для сжатия изображенийс приемлемым качеством типичными допустимыми

значениями для показателя PSNRявляются значения не меньшие 30-40 дБ. Если значение опускается ниже предельных, то такие искажения изображения становятся визуально заметными.Так как PSNR – это отношение полезного сигнала к шуму, то, чем выше значение PSNR, тем меньше визуальная заметность шума вносимого в процессе встраивания.

Полученные результаты в таблице 1 показывают, что для большинства фотореалистических изображений встраивать сообщение в старшие биты значений нецелесообразно, потому что значение показателя PSNR снижается ниже предельного значения 30 дБ, а это значит, что встроенная информация будет визуально обнаружима. При встраивании в четыре младших бита значения не опускается ниже предельного значения, что позволит использовать такой метод встраивания в случае большого объема встраиваемого сообщения. Данное допущение было принято в проводимом исследовании.

Исследование и анализ стеганоаналитических методов. Суть RS-метода заключается в том, что все изображение разбивается на группы по n значений цветовых компонентов пикселей $G(x_1,x_2,\dots x_n)$, находящихся рядом по горизонтали, где n четно. Для каждой группы определяется

Таблица 1

Показатели искажения (ПИ) при встраивании сообщения в разные биты значений цветовых составляющих пикселей

№ бита / ПИ	1	2	3	4	5	6	7	8	1&2	1&2 &3	1&2 &3 &4
PSNR (дБ)	51,13	45,11	39,09	33,09	27,04	21,10	14,89	8,70	44,16	37,90	31,79
RMSE	0,72	1,42	2,83	5,66	11,34	22,47	45,92	93,65	1,58	3,25	6,57

функция регулярности $f(G)$, рассчитанная как сумма перепадов смежных значений, где значения представляютсобой целые числа от 0 до 255.

$$f(x_1,x_2,\dots x_n)=\sum_{i=1}^{n-1}|x_{i+1}-x_i|, \quad (3)$$

где $f(x_1,x_2,\dots x_n)$- функция регулярности; x_i - значение элемента группы; n – количество элементов в группе.

Далее определяются две функции флиппинга $F(x)$: F_1, представляющая собой инверсию младшего бита значения; F_{-1}, представляющую собой инверсию с переносом в старший бит. При применении флиппинга к каждому значению группы получается две преобразованные группы значений. После чего все группы делятся на классы следующим образом:

- регулярные группы: $G\cup R\cup f(F(G))>f(G)$;
- сингулярные группы: $G\cup S\cup f(F(G))<f(G)$;
- неиспользуемые группы: $G\cup U\cup f(F(G))=f(G)$.

В дальнейшем исследуется соотношение между группами в изображении. Для этого определяется количество групп, попавших в тот или иной класс: R_1,S_1,U_1 и R_{-1},S_{-1},U_{-1}. Индексы у классов обозначают применение F_1 и F_{-1} функций флиппинга для получения распределения.

Метод основывается на статистическом предположении, что для естественного изображения, которое не подвергалось встраиванию информации, характерно следующее: $|R_1|\cong|R_{-1}|$ и $|S_1|\cong|S_{-1}|$. Предполагается, что применение функции флиппинга F_{-1} даст тоже распределение, что и функция F_1 на изображении, значение компонентов пикселей которого сдвинуты на единицу. Для изображения без встраивания соотношение между группами не должно существенно меняться, а значительное расхождение свидетельствует о применении НЗБ-встраивания.

На графике (рисунок 2) представлена разница регулярного класса между $|R_1|$ и $|R_{-1}|$, зависящая от процента встроенной информации. Видно, что при 100% заполнении изображения информацией разница между $|R_1|$ и $|R_{-1}|$ существенно возрастает для различных типов изображений и можно утверждать, что в изображение была внесена информация с помощью замены НЗБ.RS-метод реагирует на естественный шум в изображении, поэтому предположить объем встроенной информации в контейнере довольно сложно. При низком проценте встраивания информации в

изображение нельзя предположить о наличии стегановставок, а при высоком проценте встраивания — это существенно заметно.

Рассмотрим метод анализа распределения пар значений на основании критерия Хи-квадрат, использующий для анализа гистограмму, построенную по элементам изображения, и оценки распределения пар значений этой гистограммы. Метод основан на том, что младшие биты значений изображения со стегановставкой не являются случайными.

Предполагается что, частоты двух соседних элементов пустого контейнера должны находиться достаточно далеко от средних арифметических значений частот этих элементов. В контейнере со стегановставкой ситуация, когда частоты соседних элементов близки по значению, встречается достаточно часто, то есть при встраивании информации в контейнер данные частоты сближаются или становятся равными.

Для цветных BMP-изображений пары значений формируются значениями цветовых составляющих пикселов.

На основании [3], считается, что идея метода Хи-квадрат заключается в подсчете вероятности встраивания информации на основании того, как близко располагаются значения частот соседних элементов контейнеров.

Для того чтобы рассчитать вероятность встраивания информации в контейнере, необходимо рассчитать теоретически ожидаемую частоту элементов пары:

$$n_i^* = \frac{|n_i - n_{i+1}|}{2}, \tag{4}$$

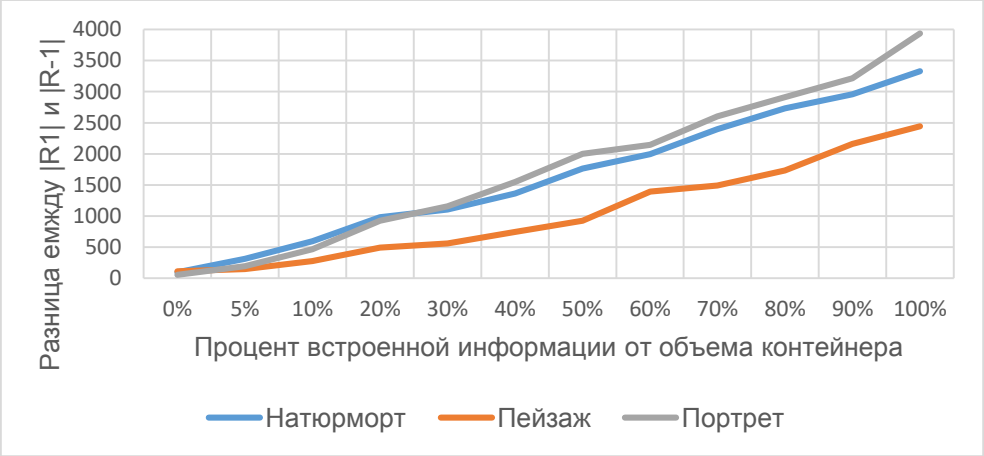


Рис. 2. График зависимости разницы между классами регулярной группыRed-компоненты различных типов BMP-изображений от процента встроенной информации

где n_i^* – теоретически ожидаемая частота появления элементов i-й пары; n_i – эмпирическая частота появления четного элемента i-й пары.

На основании вычисленных данных по формуле (5) необходимо рассчитать статистику Хи-квадрата с k-1 степенью свободы.

$$X^2_{k-1} = \sum_{i=1}^{k} \frac{(n_i - n_i^*)^2}{n_i^*}, \tag{5}$$

где X^2_{k-1} – статистика Хи-квадрата с k-1 степенью свободы; k – количество пар значений элементов контейнера; n_i^* – теоретически ожидаемая частота появления элементов i-й пары; n_i – эмпирическая частота появления четного элемента i-й пары.

После расчёта статистики Хи-квадрат по формуле (6) вычисляется вероятность встраивания секретного сообщения в контейнер.

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}}\Gamma\left(\frac{k-1}{2}\right)} \int_0^{X^2_{k-1}} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx, \tag{6}$$

где p – вероятность встраивания информации в контейнер; k – количество пар значений элементов контейнера; X^2_{k-1} – статистика Хи-квадрат с k-1 степенью свободы.

Эффективность работы метода зависит от способа встраивания информации в контейнер. Для того, чтобы данный метод работал более точно, необходимо разбить изображение на блоки и отдельно рассчитывать наборы частот элементов и вероятность скрытия для каждого блока. Также

блочный метод Хи-квадрат позволяет выбрать отдельные области изображения и проводить последующий анализ только выбранного блока.

На графике представлены результаты выполнения метода Хи-квадрат при заполнении на половину различных типов BMP-изображений стегановставкой. На графике видно, что на половине контейнера значение с 1 спускается до 0, где значение 1 означает наличие стегановставки, а значение 0 ее отсутствие. После достижения границы встроенного сообщения, вероятность встраивания начинает постепенно убывать, так как происходит накопление статистики Хи-квадрата по пустым блокам контейнера. При полном заполнении контейнера значения, полученные по отдельным блокам изображения, колеблется около 1, что означает присутствие встроенной информации, а у пустого контейнера значения приближены к 0, как показано на графике, что означает отсутствие какого-либо встраивания в наименее значимые биты контейнера.

Заключение.

Данные методы показали хорошие результаты в обнаружении стегановставки от среднего процента объема встраивания информации в изображениях различных типов: пейзажей, портретов, натюрмортов, черно-белых изображений и т.д.

Путем создания искусственного шума в изображении, два метода были проверены на возможность ложного срабатывания, но вызвать его не удалось. Так как с помощью RS-метода невозможно определить встроена ли информация при маленьком проценте встраивания, то целесообразно использовать метод в комплексе с методом Хи-квадрат или с другими методами стеганоанализа как статистическими, так и методами из других категорий.

Так же следует отметить, что эффективность работы методов в значительной степени зависит от типа изображения-контейнера, а выявление данной зависимости требует проведения дополнительных исследований.

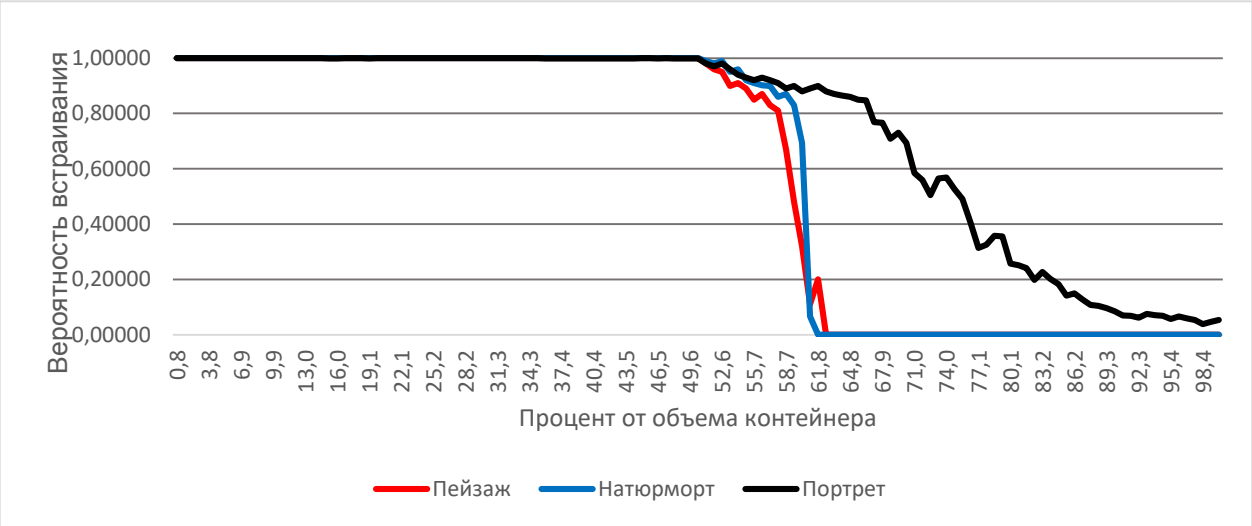


Рис. 3. График вероятности встраивания информации наполовину заполненных различных типов BMP-изображений стегановставкой, используя блочный метод Хи-квадрата

Данная работа выполнена при частичной поддержке Российского Фонда Фундаментальных Исследований РФФИ (грант 17-07-00849-А).

СПИСОК ЛИТЕРАТУРЫ

1. Fathimal, M. K Out of N Secret Sharing Scheme with Steganography and Authentication / M. Fathimal, P. Arockia Jansi Rain // Computational Intelligence, Cyber Security and Computational Models / Springer. 2016. С. 413–425.
2. Аграновский, А.В. Стеганография, цифровые водяные знаки и стеганоанализ: Монография / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. М.: Вузовская книга, 2009. 220 с.
3. Генне, О.В. Основные положения стеганографии / О.В. Генне // Защита информации / Конфидент. 2000. №3. С. 20-25.
4. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин. СПб.: СОЛОН-Пресс, 2002. 280 с.
5. Fridrich, J. Steganalysis of LSB Encoding in Color Images / J. Fridrich l, R. Du, L. Meng // тутназваниежурнала / ICME. 2000.
6. Лапшенков, Е.М. Не эталонная оценка уровня шума цифрового изображения на основе гармонического анализа / Е.М. Лапшенков // Компьютерная оптика. 2012. Т. 36. №3. С. 439-447.
7. Кошкина, Н. В. Обзор и классификация методов стеганоанализа/Н. В. Кошкина//Управляющие системы и машины, 2015. № 3 (257). С. 3-12.
8. Neil F. Johnson Steganography Software URL:http://www.jjtc.com/Steganography/tools.html (дата обращения: 20.04.2017)
9. Разинков, Е.В. Стойкость стеганографических систем/Е. В. Разинков, Р.Х. Латыпов//Ученые записки Казанского Государственного Университета, 2009. Том 151, Кн.2. С. 126-132.

УДК 004.056

ПРИМЕНЕНИЕ ЯЗЫКА PYTHON ДЛЯ РАЗРАБОТКИ СРЕДСТВ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

Никитин Андрей Сергеевич, Москвин Дмитрий Андреевич
Санкт-Петербургский политехнический университетПетра Великого
Россия, Санкт-Петербург, ул. Политехническая, 29
e-mails: annik.syn@gmail.com, moskvin@neo-bit.ru

Аннотация. Рассмотрены вопросы, связанные с разработкой эффективных средств оценки безопасности компьютерных сетей на языке программирования Python. В рамках проведенной работы разработаны вспомогательная библиотека и прототип системы оценки безопасности компьютерных сетей.

Ключевые слова: *компьютерные сети; безопасность; средства оценки безопасности; python.*

APPLICATION OF THE PYTHON PROGRAMMING LANGUAGE FOR NETWORK SECURITY TOOLS DEVELOPMENT

Nikitin Andrey, Moskvin Dmitry
Peter the Great St. Petersburg Polytechnic University,
Russia, St. Petersburg, Polytechnicheskaya str., 29
e-mails: annik.syn@gmail.com, moskvin@neo-bit.ru

Abstract. In this article we cover issues, connected with network security assessment tools development in Python programming language. Main result of our work is supplementary library and prototype of network security assessment tool.

Keywords: *computer networks; information security; network security assessment tools; python.*

Многие задачи по оценке безопасности компьютерных сетей требуют работы с сетевым трафиком на более низком уровне, чем предоставляемый традиционным интерфейсом сокетов. Примерами являются фаззинг реализации стека TCP/IP, и тестирование систем обнаружения вторжений, в ходе которого проверяется обработка фрагментированных пакетов. Обязательным условием для выполнения таких задач является возможность генерации сетевых пакетов в обход сетевого стека.

Для современных операционных систем существуют технологии, предоставляющие возможность низкоуровневой работы с сетевыми интерфейсами. В число встроенных механизмов, доступных в операционных системах семейства UNIX, входят сырые сокеты, и библиотека pcap с необходимой поддержкой на уровне ядра. На ОС семейства Windows для этой цели доступны адаптированные версии библиотеки pcap - WinPcap и Npcap - поставляющиеся с соответствующими сетевыми драйверами.

Как правило, приложения, работающие с сетевыми пакетами, реализуют на компилируемых языках, таких, как C, C++. Причин такого выбора могут являться требования к производительности приложений и доступность API применяемых технологий. Однако, за счет большего удобства разработки, хорошим выбором являются интерпретируемые языки [1], в число которых входит Python. Наличие ряда библиотек [2, 3] для работы с сетевым трафиком демонстрирует востребованность данного языка в области сетевой безопасности.

Наше исследование показывает, что Python можно применять для разработки приложений, реализующих низкоуровневые операции с сетевым трафиком, и имеющих достаточную производительность для экспериментальной проверки новых идей, и применения в качестве завершённых программных продуктов. В рамках исследования на основе pcap разработана библиотека для языка Python 3, позволяющая выполнять генерацию, отправку, получение и анализ сетевых пакетов. Библиотека использует только средства стандартной библиотеки языка, и не зависит от модулей на других языках. Библиотека использована при разработке прототипа системы оценки безопасности компьютерных сетей, включающей в себя функции сканирования портов, классификации узлов сети по параметрам ответных пакетов, сбора баннеров сетевых сервисов, проверки слепых SQL-инъекций. Полученная система обладает достаточной эффективностью для решения различных задач, связанных с информационной безопасностью.

СПИСОК ЛИТЕРАТУРЫ

3. Макконнелл С. Совершенный код. Мастер-класс / Пер. с англ. - М.: Издательство «Русская редакция», 2010. - 896 стр.
4. Scapy // SecDev.org. URL: http://www.secdev.org/projects/scapy/ (дата обращения: 23.09.2017).
5. libdnet // libdnet. URL: http://libdnet.sourceforge.net/ (дата обращения: 23.09.2017).

УДК 681

ЭКОЛОГИЧЕСКИЙ КОНТРОЛЬ И РАЗВИТИЕ МОДЕЛЕЙ ПОПУЛЯЦИОННОГО РОСТА

Павлова Светлана Михайловна
Смольный университет Российской академии образования
Россия, Санкт-Петербург, Полюстровский пр., 59
e-mail: spavlova222@mail.ru

Аннотация. В статье рассматривается экологическийконтроль, который определяет особую актуальность обеспечения объективности и достоверности получаемой в процессе мониторинга информации. Ведь любое решение становится полезным и оптимальным, только когда оно основано на объективных и достоверных данных. Эта проблема понимается широким кругом ученых и практиков, связанных с философскими, математическими и информационными вопросами природоохранной и природопользовательской деятельности. Для более общих задач статистического мониторинга свойств сложного объекта, ориентированного на его специфику. При этомЭС «АССИСТЕНТ» выступает в качестве базового модуля.

Ключевые слова: *экспертная система; информационно-измерительные системы; мониторинг; лингвистические шкалы; байесовские интеллектуальные измерения.*

ENVIRONMENTAL CONTROL AND DEVELOPMENT OF MODELS OF POPULATION GROWTH

Pavlova Svetlana
Smolny university of the Russian Academy of Education
Russia, St. Petersburg, Polyustrovsky pr., 59
e-mail: spavlova222@mail.ru

Abstract. The article presents tasks define a special urgency to ensure the objectivity and reliability of the resulting data in the monitoring process. After all, any decision becomes a useful and optimal one only when it is based on some objective and reliable information. This problem refers to a wide range of scholars and practitioners associated with the philosophical, mathematical and informational issues on environmental and natural activities for more general problems of statistical monitoring of the properties of a complex object, based on its specific character. In this case ES "ASSISTANT" acts as a basic module.

Keywords: *expert system; information and measuring systems; monitoring; linguistic scales; Bayesian linguistic measurements.*

Введение.Важность задачи мониторинга определяет особую актуальность обеспечения объективности и достоверности получаемой в процессе мониторинга информации. Ведь любое решение становится полезным и оптимальным, только когда оно основано на объективных и достоверных данных. Эта проблема понимается широким кругом ученых и практиков, связанных с философскими, математическими и информационными вопросами природоохранной и природопользовательской деятельности. Для более общих задач статистического мониторинга свойств сложного объекта, ориентированного на его специфику. При этом ЭС «АССИСТЕНТ» выступает в качестве базового модуля.

1.1. Теоретическое обоснование регуляризирующего байесовского подхода.

Одним из способов повышения степени устойчивости решений является ограничение пространства возможных решений путем формирования системы дополнительных ограничений, приводящих к созданию компактного пространства устойчивых решений [1,3].

Основная идея регуляризирующего байесовского подхода (БРП) состоит в привлечении измерительного подхода в процесс байесовского оценивания путем применения шкалирования, метризующего пространство байесовских решений. Получение результатов ИИ на компактах иерархических (согласно структурам ОИ и ВФ) метрических шкал, согласно теореме Тихонова [3], обеспечивает их устойчивость в пределах этих компактов. Таким образом, введение измерительной шкалы, обусловливая дополнительные ограничения на пространство возможных решений, оказывает регуляризирующие действия, что обосновывает название данной модификации байесовского подхода и позволяет ввести задачу ИИ на основе РБП в класс условно-корректных по Тихонову. Алгоритмы ИИ, реализующие такую идейную основу, будут обладать регуляризирующими свойствами при проведении измерений в сложных измерительных ситуациях при значительной априорной неопределенности информации об ОИ и ВФ. Интеллектуальные измерения, реализуемые на основе РБП, назовем байесовскими интеллектуальными измерениями (БИИ). Для построения алгоритмов БИИ необходимо определить их принципиальную основу, которая характеризуется уравнением измерений.

1.2. Концепция шкалы с динамическими ограничениями.

Понятие абстрактной измерительной шкалы дано в работах [3,4], которое определяет шкалу как совокупность правил, позволяющих выполнить гомоморфное преобразование Ψ для отображения реляционной системы объекта G в знаковую систему шкалы (в частности, в числовую),

представляющую собой реляционную систему GS со свойствами $\left\{Q_{i_{G_S}}\right\}$ и отношениями $\left\{W_{j_{G_S}}\right\}$, $i_{G_S} = 1, I_{G_S}; j_{G_S} = 1, J_{G_S.}$ (1)

1.3. Основные свойства шкалы БИИ.

В измерительной практике используются разнообразные по измерительной мощности шкалы, теоретическому обоснованию и приложениям которых посвящены работы [3]. Наиболее полная их классификация приводится в литературе [3] по репрезентативной теории измерений, которая успешно развивается в настоящее время. В соответствии с нею все разнообразие шкал составляет несколько групп, к которым относятся шкалы наименований, порядка, интервалов, отношений, абсолютные, функциональные и др. В зависимости от их метрологических свойств они подразделяются на метрические и неметрические.

Метрические шкалы позволяют определять расстояние между соседними реперами носителя шкалы и организуются в метрическом пространстве результатов измерений — реперов шкалы. Неметрические шкалы [3] организуются на множестве элементов носителя шкалы, для которого понятие метрики (расстояния), как правило, не определено. К таким шкалам относятся шкалы наименований и порядка, для которых определены отношения эквивалентности (эквивалентности и порядка). Носители таких шкал могут быть представлены в виде лингвистических множеств. Эти шкалы используются в задачах классификации, распознавания, таксономии для принятия решений. Отсутствие метрических свойств в этих шкалах и целого ряда отношений, необходимых для реализации ШДО, не позволяет принять их в качестве основы для построения нового типа шкал БИИ.

1.4. Принципы синтеза шкал ШДО БИИ.

Построение любой измерительной шкалы начинается с формирования носителя шкалы, представляемого дискретным множеством результатов измерений $\{h_k\} \in H_K$, принятых в качестве представителя градаций $\{q_i^*\}$ измеряемого свойства q. Это позволяет рассматривать множество НК как подмножество множества нешкалированных возможных результатов Н. При соблюдении условий (1) множество НК реперов шкалы неплотно покрывает множество Н, а система носителя шкалы GS является фрагментом или подсистемой системы, соответствующей множеству результатов Н. Для реализации измерительной шкалы пространство ее носителя НК должно быть метрическим, для которого определено понятие меры близости между отдельными элементами носителя шкалы. Тогда каждой паре hi, hj элементов носителя шкалы должно соответствовать вещественное число $p_i = p(h_i, h_j)$, удовлетворяющее аксиомам расстояния:

– неотрицательности:

$p(h_i, h_j) = 0 \Leftrightarrow h_j = h_i;$ (2)

– симметрии:

$p(h_i, h_j) = p(h_j, h_i);$ (3)

– треугольника:

$p(h_i, h_z) \le p(h_i, h_j) + p(h_j, h_z).$ (4)

1.5. Концепция и принципы построения сопряженной лингвистической шкалы БИИ.

Не менее важную часть априорной информации, особенно в условиях измерительной ситуации БИИ, представляют собой сведения о лингвистической форме: естественно научные знания, наблюдения в форме описаний, аналоги из других предметных областей, лингвистические оценки экспертов, а также решения, выводы и рекомендации относительно ОИ, которые были получены ранее.

Для обработки и принятия решений на основе подобной информации развиты специальные теории: лингвистических переменных [3,4], теории возможностей, ситуационного управления и др. Основой формализации такой информации в данных теориях является аппарат теории нечетких множеств, позволяющий отображать имеющуюся информацию в виде специальных функций — функции принадлежности $\mu(\nu \mid x)$, которой придается следующий смысл:

$\mu(\nu \mid x) \in M_{\text{Б}} \cdot (\nu \mid x) \in [0; 1],$ (5)

где $\text{Б}^* = \{\langle M_{\text{Б}} \cdot (x) | x \rangle\}$ — нечеткое множество множества X, а X — базовое множество или базовая шкала значений контролируемого свойства ОИ. Носителем Б нечеткого множества Б^* на такой шкале являются те элементы X, для которых значения функции принадлежности отлично от нуля: (1)

$\{MX(t_l)\}_k^n = \{MX(t_l)\}_k^n \mid \{MX(t_l)\}_k^{an} \mid \{MX(t_l)\}_x) * \{MX(t_l)\}_k^{an} * \{MX(t_l)\}_x \mid \text{У}_i^{\text{п}}(t_l).$ (6)

2. Концептуальная основа параметрических байесовских интеллектуальных измерений.

Этап синтеза лингвистических параметрических шкал БИИ проводится в соответствии с методологией и по формулам (1,2) которые для лингвистического представления информации не имеют специфики в параметрических БИИ и поэтому не повторяются. Уравнение ПБИИ приведено далее в виде (3).

Если алгоритм ПБИИ состоит из нескольких этапов измерительных преобразований, то он реализуется в виде цепочки этапов ПБИИ.

Для статистик такими этапами алгоритма БИИ являются, как правило: этап их вычисления по эмпирическим данным по алгоритму $\varphi_{\text{ст}}$ и этап последующего шкалирования оценки статистики по алгоритму φ_s. Тогда ПБИИ принимает косвенных ПБИИ, для которых: (2)

– $\{h_k(x,t)|P_k(t)\} = \text{argmin}\text{C}_\text{B}\psi_h^\text{п}(x_i(t),t)|\psi_h^{a\text{п}}(A(t),t)|\text{У}_i^\text{п} =$
$\text{argmin}\text{C}_\text{B}\psi_s^\text{п}(\psi_{\text{ст}}^\text{п}(x_i(t),t),t)|\psi_h^{a\text{п}}(A(t),t)|x_i(t)|\text{У}_i^\text{п}(t);$ (7)

– КМХ результата (3):

– $\{MX(x,t)\}_t = \{MX(t)\}_s^\text{п} * \{MX(t)\}_{\text{ст}}^\text{п} * \{MX(t)\}_x|h_k(x_i,t);$ (8)

– условная погрешность БИИ статистики (3):

$f(\Delta h_k^\text{п}(t)|\, h_k^\text{п}) = f(\Delta h_{Sk}^\text{п}(t)) * f(\Delta h_{\text{стк}}^\text{п}(t)) * f(\Delta x_i(t))| * f(\Delta h_k^{a\text{п}}(t))|\text{У}_i^\text{п}(t).$ (9)

Алгоритм ПБИИ синтезируется вновь при меняющихся во времени условиях измерения и поступающей информации. При этом меняется и все множество алгоритмов ПБИИ $\Phi_j^\text{п}(t)$.

Возможна различная форма априорной параметрической неопределенности, соответствующая следующим ситуациям:

– какой-либо априорной информации о значениях или их диапазонах для параметра, а также априорного и точного выборочного распределения параметра нет;

– имеется информации о диапазоне изменения параметра, однако нет информации об априорном распределении значений параметра;

– имеется информация, достаточная для определения области распределения параметра, его априорного распределения и точного выборочного распределения параметра.

Если вид точного выборочного распределения статистики неизвестен, то его определяют либо путем аналитических преобразований, либо путем имитационного моделирования, либо принимают равномерно распределенными выборочными значения статистики. Алгоритм определения выборочного распределения статистики входит как подэтап преобразования в алгоритм $\varphi_{\text{ст}}$(t). Очевидно, что с накоплением информации вид точного выборочного распределения может уточняться.

При первой ситуации на начальном этапе шкала строиться от оценки статистики $\widetilde{h_k}(t_1)$. Альтернативные решения располагаются справа и слева от нее на расстоянии $\rho(\varepsilon_{\text{доп}})$. В процессе измерений шкала развивается и достраивается, определяя истинный диапазон изменения параметра.

Для второй ситуации возможно построение универсальной параметрической шкалы БИИ, в которой элементы носителя шкалы выражены в относительных, приведенных к концу шкалы значениях.

Видно, что вид распределения вероятностей значений параметра может существенно повлиять на вид носителя шкалы БИИ. При неравновероятном априорном распределении параметра интервалы между соседними элементами носителя шкалы оказываются также неравномерными. Преимущества имеют элементы с меньшей априорной вероятностью.

Синтез алгоритмов ПБИИ статистик математического ожидания, дисперсии, коэффициентов асимметрии и эксцесса рассматривается в работах выше.

2.1. Алгоритмы БИИ статистик проверки статистических гипотез.

Можно показать, что задачи проверки статистических гипотез входя в класс задач измерительного контроля БИИ: (4)

$\{h_k|P_k\} = \psi^{\text{пр}}\left(\psi_j^\text{о}|x_i|\text{У}_i^o\middle|\text{У}_i^{\text{пр}}\right);\ \psi_j^{\text{пр}} \in \psi_\text{J}^{\text{пр}};\ \psi_j^o \in \psi_\text{J}^\text{о},$ (10)

где $\psi^{\text{пр}}$, $\psi_\text{J}^\text{о}$ — алгоритмы БИИ принятия решений по критерию ω и оценивания соответственно.

Обобщенный алгоритм проверки статистических гипотез $\theta_i \in \theta_I$ по критерию $\omega(\theta_I, x)$ может быть представлен в виде:

$\theta = \theta_0 \leftrightarrow \hat{\theta} = \arg(P(\,\hat{\theta}(x)|\theta_0\,) = a_{\text{доп}}),$ (11)

где $\text{P}(\tilde{\theta}(x))$ — интегральный распределения статистики $\tilde{\theta}(x)$, $a_{\text{доп}}$ — уровень значимости критерия.

Можно переписать выражение для критерия в виде последовательности функциональных преобразований оценивания статистики $\varphi^{\text{ст}}$ и принятия решения по критерию φ^ω:

$\theta = \psi^\omega(\psi^{\text{ст}})(x|\theta_0, a_{\text{доп}}).$ (12)

2.2. Измерительные задачи мониторинга сложных технических и природных объектов

К одним из самых наукоемких и технически сложных задач относятся задачи мониторинга сложных объектов. Понятие сложного объекта как объекта, полностью определяемого своими свойствами и отношениями между ними и другими объектами, составляющими среду функционирования приведены в [3]. К числу сложных объектов относятся объекты, активно взаимодействующие со средой, свойства и отношения между которыми неизвестны точно. Основными свойствами сложных объектов мониторинга являются [3]:

– естественная иерархичность структуры объекта, подтверждаемая созданными человечеством классификационными системами (например, для природных объектов классификации видов живых организмов — система Менделеева, иерархия слоев околоземного пространства, планетарная структура Солнечной и других космических систем и др.);

– существование реальных признаков, определяющих принадлежность характеристик объекта к тому или иному уровню иерархии структуры объекта;

– взаимосвязанность иерархических уровней, составляющих объект как единое целое, отражающая взаимосвязь характеристик объекта;

– невозможность точного формализованного описания объекта;

– уникальность объекта, обусловливающая трудности представления типового образа объекта;

– невозможность или нежелательность по каким-либо причинам экспериментов над ним как над источником информации при изучении или моделировании его свойств;

– значительная часть информации о таком объекте обычно содержится в форме сведений, наблюдений, рекомендаций, описания ситуаций и фактов из опыта общения с ним человека, представленных в семантической форме;

– распределенность объекта во времени и географическом пространстве;

– устойчивость, саморегуляция и самоорганизуемость при меняющихся условиях функционирования.

Примерами таких объектов могут быть технические системы, состоящие из ряда подсистем, характер взаимодействия которых не может быть определен точно доступными средствами, искусственные объекты, активно взаимодействующие со средой их функционирования, а также все природные объекты.

Понятие мониторинга для сложных объектов искусственного происхождения дано в [5]. Оно определяет мониторинг как процесс слежения за состоянием объекта и сопоставления его текущего состояния с контрольными образцами (уровнями или точками).

Термин «мониторинг» как понятие для природного объекта был впервые введен в использование на Стокгольмской конференции в 1972 году. После этого начали активно развиваться два направления мониторинга природных объектов, которые принципиально отличались друг от друга принятием и отрицанием функции регулирования (управления) природным объектом.

Так, в первой концепции мониторинг природного объекта понимается как процесс сбора, хранения, преобразования экспериментальной информации об объекте мониторинга и выработке регулирующего воздействия, направляемого на объект по линиям обратной связи. В определение понятия мониторинга во втором направлениивключаются все перечисленные подзадачи первого направления, кроме последней. Конечной целью мониторинга при этом считается выработка рекомендаций в поддержку тех или иных решений, оптимальных с точки зрения принятых критериев.

При втором главной целью мониторинга считается контроль состояния объекта при всемерном и всестороннем его познании и управлении процессом этого познания, а также выработке рекомендаций по регулированию антропогенного влияния, что обеспечивает, в конечном итоге, устойчивое развитие объекта.

Важность задачи мониторинга определяет особую актуальность обеспечения объективности и достоверности получаемой в процессе мониторинга информации. Ведь любое решение становится полезным и оптимальным, только когда оно основано на объективных и достоверных данных. Эта проблема понимается широким кругом ученых и практиков, связанных с философскими, математическими и информационными вопросами природоохранной и природопользовательской деятельности. Как отмечается в работе Н. Н. Моисеева [2,5], «Объективность получаемых знаний — важнейший вопрос планетарной экологии». В работе отмечается важность задачи мониторинга и получения достоверной информации для обеспечения устойчивого развития экосистем, в том числе и в России. Реализация принципов и стратегических требований всемирных форумов в 1992 году в Рио-де-Жанейро и в 1994 году в Манчестере, сформулированных в «Декларации» и «Повестке дня XXI века», а также в обращениях и докладах их участников, возможна только на основе формирования современной информационной цивилизации, базирующейся на новых методах и средствах получения точных и достоверных знаний об окружающей природной среде.

Таким образом, эффективно решить задачи мониторинга сложных объектов в сложных измерительных ситуациях и использовать результаты мониторинга для обеспечения устойчивого функционирования сложных природных или технических систем можно только с позиций измерительного подхода на принципах единства измерений и при постоянном метрологическом обосновании получаемых результатов.

Процесс реализации информационно-измерительных систем мониторинга предполагает выбор методической, информационной и технической баз ИИС. Специфика задач мониторинга сложных объектов предъявляет такого рода ИИС определенные требования, которые на основании приведенных выше рассуждений можно выразить следующим образом:

– в процессе мониторинга должно обеспечиваться познание объекта мониторинга (ОМ);

– решение задачи мониторинга должно производиться на основе всей доступной априорной информации об объекте мониторинга и среде его функционирования и информации, получаемой в процессе измерительного эксперимента;

– все получаемые промежуточные и окончательные результаты мониторинга должны иметь метрологическое обоснование в виде показателей их качества;

– для эффективного решения задач мониторинга модели объектов и СФ, а также методы, алгоритмы и средства мониторинга должны отражать основные свойства сложных объектов (в частности, свойства устойчивости, саморазвития и самоорганизации);

– результаты мониторинга должны быть представлены в формах значений параметров, аналитических выражений, выводов и решений, представленные в лингвистической форме.

Для более общих задач статистического мониторинга свойств сложного объекта, ориентированного на его специфику. При этом ЭС «АССИСТЕНТ» выступает в качестве базового модуля.

2.3. Экспертная система «АССИСТЕНТ» для статистического мониторинга сложных объектов

ЭС «АССИСТЕНТ» в настоящее время является основой нескольких ЭС для статистического мониторинга технических, искусственных и природных объектов, среди которых ЭС «АССИСТЕНТ-КЛАСС» для классификации технических и природных объектов по изображению, «АССИСТЕНТ-МЕТРОЛОГ» для метрологической исследовательской аттестации средств измерений, «АССИСТЕНТ-ГИДРОЛОГ» для мониторинга акваторий, «АССИСТЕНТ-ИХТИОЛОГ» для оценки состояния и характеристик рыбных ресурсов, «АССИСТЕНТ-БИОЛОГ» для биосферного мониторинга экосистемы и др. Кроме того, ЭС «АССИСТЕНТ» применялась в задачах статистической обработки и мониторинга технологических производственных процессов, сложных перерабатывающих комплексов и стала интеллектуальной средой в виде ЭС «АССИСТЕНТ-ЭКОЛОГ» [3,4] в ИНИИС для оценки состояния атмосферы.

Заключение.

Однако, хотя к решению задач мониторинга в настоящее время привлечены усилия многих ученых и организаций, многочисленные методические и технические средства, получение объективной информации, достаточной для познания закономерностей развития природной среды и функционирования сложных объектов, а также для принятия оптимальных решений экологического управления, остаются недоступными и по сей день. Основными причинами этого являются сложность самих объектов мониторинга, отсутствие эффективных методов и средств получения информации, ориентированных на специфику сложных объектов и метрологического обеспечения результатов мониторинга, субъективность окончательных решений о состоянии объекта, что при несомненной целесообразности использования опыта специалистов не позволяет обобщить весь объем полученной информации и вносит ошибки в результаты мониторинга.

СПИСОК ЛИТЕРАТУРЫ

1. Мэгарран Э. Экологическое разнообразие и его измерение. – М.: Мир, 1992.- 368 с.
2. Лебедев А.Н. Модели сложных объектов. – Пенза: ППИ, 1977. – 71 с.
3. Д.Д. Недосекин, Е.А. Чернявский и др. Информационные технологии интеллектуализации измерительных процессов.- СПб.; Энергоатомиздат. Санкт- Петербургское отделение, 1995.- 178 с .: ил. ISBN 5-283-04706-76
4. Павлова С.М. Становление и развитие моделей популяционного роста/ С.-Петербург.электротех.ун-т.- СПб.,1996.- Деп. В ВИНИТИ 28.05.96, №1721-В96.
5. В.Е. Болтнев Экология.- Издательство : ТНТ 2012.- 352. – ISBN9785941782581

УДК 004.04+658.5

МОДЕЛИРОВАНИЕ СЛОЖНЫХ МАШИНОСТРОИТЕЛЬНЫХ ИЗДЕЛИЙ В ХОДЕ ПРОИЗВОДСТВЕННЫХ ИСПЫТАНИЙ

Первухина Елена Львовна, Осипов Константин Николаевич, Голикова Виктория Викторовна
Севастопольский государственный университет Россия, Севастополь
ул. Университетская, 33
e-mails: pervukhina14 @mail.ru, assistenttmm@mail.ru, golikova.victoria@gmail.com

Аннотация. Ранее предложенный авторами метод моделирования сложных машиностроительных изделий в ходе их производственных испытаний анализируется в контексте теории квалиметрии моделей сложных объектов.

Ключевые слова: *моделирование; квалиметрия моделей; сложные машиностроительные изделия; производственные испытания.*

MODELINGOFTHE COMPLEX MACHINES DURING THEIR ACCEPTANCE TESTING

PervukhinaElena, Osipov Konstantin, Golikova Victoria
Sevastopol State University, Russia, Sevastopol, Universitetskay str., 33
e-mails: pervukhina14 @mail.ru, assistenttmm@mail.ru, golikova.victoria@gmail.com

Abstract. The method of complex machine modeling, which is previously proposed by the authors, is analyzed in the context of the model qualimetry theory.

Keywords: *modeling; model qualimetry; complex machine-building products; production tests.*

Введение. В связи с ужесточением требований к качеству, в том числе надежности, современных сложных машиностроительных изделий, расширением номенклатуры технических операций, усложнением и ростом разнообразия их конструктивных элементов и различий в условиях эксплуатации, задача совершенствования методов оценки технического состояния и контроля качества в ходе стендовых приемосдаточных испытаний перед сдачей в эксплуатацию продолжает оставаться актуальной, несмотря на появление автоматизированных стендов со встроенным программным обеспечением (ПО). Как правило, используемые традиционные методы оценки состояния изделий не позволяют оперативно определять скрытые производственные дефекты и неисправности в течение ограниченного времени испытаний по ограниченному числу измеряемых параметров, особенно при стремлении производителей снизить расходы на испытания. Достижение требуемой для повышения конкурентоспособности продукции отечественного машиностроения достоверности и точности результатов испытаний при снижении расходов на них требует новых методов оценки технического состояния.

В научно-технической литературе последних лет присутствуют примеры методов и алгоритмов оценки состояния сложных машиностроительных изделий [1, 2]. Однако большинство из них уникально и не может быть использовано в массовом и серийном производстве, в том числе, из-за большой сложности предлагаемых моделей и, как следствие, необходимости измерять значительное число параметров и обрабатывать большой объем информации, что снижает точность и достоверность результатов испытаний и увеличивает их стоимость [3]. Операторам испытаний представляется информация только о состояниях отдельных параметров испытуемых изделий. Интегральную оценку их состояния и принятие решений относительно их годности к эксплуатации до сих пор должны выполнять квалифицированные операторы.

Цель работы. Целью работы является анализ ранее предложенного авторами метода оценки технического состояния современных машиностроительных изделий в ходе производственных (приемосдаточных, контрольных) испытаний как основы перспективных программ испытаний в контексте развиваемой в последнее время группой российских ученых теории квалиметрии моделей сложных объектов и выбор направлений его развития.

Особенности производственных испытаний сложных машиностроительных изделий и задачи их моделирования. Под сложными машиностроительными изделиями понимаются машины и механизмы сложной структуры, состоящие из большого числа конструктивно отличающихся узлов и элементов с различными принципами и условиями функционирования, рабочими процессами различной физической природы, с большим числом связей, аналитическое описание которых невозможно. Технологический процесс испытаний, представляя элемент системы управления, является этапом получения первичной информации при контроле качества. В ходе производственных (приемосдаточных, контрольных) испытаний происходит приработка деталей, т.е. интенсивное изменение микрогеометрии сопрягаемых поверхностей деталей в подвижных кинематических парах, проверяется работа систем смазки, питания и охлаждения. В предположении отбраковки до начала сборочного процесса бракованных деталей на стадии испытаний определяют качество сборки, проверяют соответствие технических характеристик изделий ГОСТ Р или ТУ и принимают решения об их годности к эксплуатации. Эмпирическая информация о текущих состояниях испытуемых изделий имеет вид последовательных значений диагностических параметров; отражающих рабочие процессы изделий в зависимости от условий функционирования; управляющих воздействий; характера обработки, передачи и хранения данных [4].

Полное математическое описание подобных объектов является трудной научной задачей. С точки зрения концепции создания интеллектуальных информационных технологий мониторинга [5-7], для комплексного моделирования сложных технических систем и объектов нужно учитывать: размерность их характеристик, многофункциональность, нелинейность и непредсказуемость поведения, его детерминированный и стохастичный характер, отсутствие полной информации об объекте в целом. Однако моделирование не является основной целью анализа измерительной информации. В общем случае, она заключается в получении обобщенных оценок совокупности параметров, значения которых подтверждают готовность изделия к эксплуатации либо указывают на деталь и вид дефекта, либо обеспечивают прогноз состояния с заданной точностью и интервалом прогноза и т.п. [8].

Моделирование представляет только этап исследования при управлении испытаниями или решения другой задачи, предполагающей оценку и прогнозирование технического состояния испытуемых изделий и динамику их функционирования. Модели должны отражать исследуемые свойства машин, полное отображение всех технических свойств не является обязательным. По определению работы [6], под результативностью моделирования понимается способность моделей давать конкретный целевой эффект. Это утверждение дает основание не добиваться полного, всеобъемлющего описания сложных объектов.

В научной литературе последних лет появились работы, предлагающие использовать статистические методы обработки измерительной информации, а также моделирования и анализа изменяющихся показателей машин для отслеживания динамики их технического состояния. Это

направление параметрической диагностики в отдельных работах называют тренд-анализом [9, 10]. Оно предполагает систематический контроль технического состояния и уровня надежности эксплуатируемого множества однотипных машин с учетом особенностей их применения, в том числе на основе статистических данных, для определения тенденций изменения значений параметров машин и выявления их возможных отклонений от нормальных значений. Главным недостатком этих работ является контроль изменения скалярных величин – отдельных диагностических показателей изделий, а также использование традиционных статистических методов и критериев, которые могут дать ошибочные результаты в случае изменения наблюдаемых случайных величин, коррелированных между собой. Поэтому тренд-анализ дополняет, а не заменяет существующие методики анализа и не может без учета всего множества диагностических параметров дать полную и достоверную картину наличия или развития неисправностей или дефектов.

Предлагаемый подход к моделированию. Для решения конкретных задач испытаний, как показано в работах авторов [4, 11], моделирование даже конструктивно сложных машин и механизмов в условиях неполной и нечеткой априорной информации об их техническом состоянии возможно современными методами многомерного статистического анализа с построением причинно-следственных зависимостей между диагностическими и структурными параметрами, отражающих динамику состояния изделий. Последние напрямую отражают техническое состояние изделий и качество сборки, (величина зазоров в сопряжениях, качество уплотнений, натяжение в резьбовых соединениях и т.д.), однако их измерение после сборки невозможно.

На первом этапе моделирования определяются наиболее информативные с точки зрения целей испытаний параметры испытуемых изделий. Под информативностью параметра понимается степень снижения неопределенности знаний о техническом состоянии испытуемых изделий после использования информации о его значениях по результатам испытаний.

Снизить расходы на испытания без снижения достоверности и точности решений, принимаемых по результатам испытаний обработки информации, можно, минимизируя множество контролируемых параметров и точек съема информации. Это особенно актуально, когда наиболее информативные параметры не поддаются измерению либо соответствующие технические возможности их измерения сдерживаются экономическими факторами.

Процесс испытаний может быть описан следующей совокупностью характеристик: {X, Y, U, W, S, **ξ**, V, MSt,T, Rst,T, RΣt,T}, где X={x1,…xn} – ненаблюдаемые параметры, Y={y1,…ym} – наблюдаемые показатели испытуемого изделия, U={u1,…up} – характеристики условий внешней среды; W={w1,… wq} – неконтролируемые действующие возмущения; S – множество точек съема информации; V – вектор движения точек съема информации (постоянное их местонахождение – частный случай); MSt,T $\in M$ – математическая модель, связывающая информативные параметры на основе наблюдаемых данных; RS – частное решение, принимаемое по MS; RΣ – окончательное решение на основе уточненной модели; t, T – время наблюдения и время принятия решения о состоянии изделия, его параметрах и характеристиках; **ξ** – способы представления информации.

Существуют разные классические метрики для выбора информативности параметров и проверки качества моделей [6]. Мы предлагаем использовать для этой цели информационный критерий, известный в литературе как дивергенция, или информационное расхождение Кульбака-Лейблера. Выбор информативных параметров и точек съема информации удобно проводить на основе информационного критерия путем определения множества признаков, свойства которых позволяют максимизировать различия между состояниями испытуемого изделия [12].

Оператор испытаний получает измерительную информацию о значениях параметра в виде k-мерного вектора $y_q = (y_1 \cdots y_k)$, $q = 1 \cdots m$, где k – число точек съема информации, и вектор измерений характеризует состояние ξ_i из конечного множества состояний изделия. Принимается допущение, что априорные вероятности каждого состояния одинаковы, т.е. вектор y_q может с равной вероятностью относиться как к одному, так и к другому состоянию; $p_i(y_q)$ – плотность распределения для вектора y_q при условии, что он передает состояние ξ_i.

Определяются инвариантные свойства возможных состояний, которые используются для понижения размерности вектора измерений. Элементы вектора (множества) выбираются на основе значений информационного критерия, выступающего в качестве меры расстояния между различными состояниями испытуемого изделия; оценивается эффективность разделения этих состояний. Выбираются элементы, которым соответствуют наибольшие значения информационного критерия, т.к. они заключают в себе максимум различающей информации. Элементы, вклад которых в информационный критерий невелик, исключаются из рассмотрения.

Задача понижения размерности вектора $y_q = (y_1 \dots y_k)$ решается определением матрицы, преобразующей исходный вектор в вектор с элементами, максимизирующими расстояние между состояниями. Информация, отличающая состояние ζ_1 от состояния ζ_2, рассчитывается с помощью логарифма отношения правдоподобия $\ln \frac{p_2(y)}{p_1(y)}$. При этом средняя различающая информация для состояния ζ_2 определяется выражением

$$I(2,1) = \int_y p_2(y) \ln \frac{p_2(y)}{p_1(y)} dy .$$

Информационное расхождение Кульбака-Лейблера

$$J(1,2) = I(1,2) + I(2,1) = \int_y [p_1(y) - p_2(y)] \ln \frac{p_1(y)}{p_2(y)} dy$$

представляет полную среднюю информацию для различения двух состояний изделия ζ_1 и ζ_2, характеризующихся плотностями распределения $p_1(y)$ и $p_2(y)$ [12].

Следующий этап моделирования изделий предполагает определение причинно-следственных зависимостей между параметрами. При анализе эмпирической информации, поступающей в виде случайных последовательных значений диагностических параметров; отражающих рабочие процессы изделий, определение таких зависимостей проводится с использованием статистических тестов, например, теста К. Грейнджера на каузальность (причинность) [4, 11]. Согласно тесту, переменная x_t является каузальной по отношению к переменной y_t (обозначается $x_t \rightarrow y_t$), если при прочих равных условиях значения y_t могут быть предсказаны по значениям x_t, измеренным ранее, с меньшей ошибкой, чем без их использования. Для проверки гипотезы «x_t не влияет на y_t» (где x_t, y_t – скалярные процессы) оценивается справедливость зависимости y_t от последовательности значений y_t и x_t. Тест позволяет однозначно выявить динамическое взаимодействие между диагностическими параметрами в виде направлений причинно-следственных связей и наряду с другими алгоритмами определяет выбор наиболее информативных параметров испытуемых изделий. При этом для исправных изделий изменение одного из параметров в одинаковых условиях испытаний должно сопровождаться изменением всех остальных.

Использование результатов моделирования для решения задач испытаний. На стадии приемосдаточных испытаний измеренные значения диагностических параметров представляют нестационарные случайные процессы даже при работе изделий на установившихся режимах. Для исправных изделий нестационарные случайные процессы изменения значений основных диагностических параметров связаны линейными комбинациями с коэффициентами, являющимися стационарными случайными величинами. Различие технических состояний отражается в изменении вероятностных характеристик случайных процессов изменения диагностических параметров. При дефектах или неисправностях значения диагностических параметров, как правило, отклоняются от номинальных значений. Стандартные характеристики функционирования изделий также отклоняются от номинальных, происходит изменение статистических связей между параметрами. В этих случаях зависимости между нестационарными процессами изменения диагностических параметров теряют стационарный характер, меняются значения коэффициентов зависимостей. Такие ситуации отличаются от тех, когда изменения вызваны только сменой режима работы испытуемых изделий. Показано [11], что для исправных изделий статистические зависимости между параметрами не нарушаются.

Математическое обеспечение автоматизированных испытаний при описанном подходе к обработке измерительной информации ориентировано на представление оператору испытаний новой информации об изменении причинно-следственных зависимостей между диагностическими параметрами изделий. Определение динамики коэффициентов этих зависимостей составляет основу многомерной модели развития свойств испытуемых изделий, проверка стабильности зависимостей – основу информационной технологии для оперативной оценки их состояния.

На следующем этапе анализа проверяем свойства моделей: устойчивость, чувствительность, наблюдаемость, робастность. Для проверки гипотезы об адекватности модели измерительной информации используются статистические тесты следа, максимального собственного числа и т.д. Несмотря на многомерность, при ограниченном числе параметров модели просты для машинной реализации и интерпретации [13]. Модели могут быть дополнены детерминированными моделями, в том числе построенными по результатам спектрального анализа, что особенно актуально при испытаниях сложных машин на неустановившихся режимах [11].

Для окончательной проверки оптимальности полученных оценок параметров испытуемых изделий вновь используется информационное расхождение Кульбака [12], согласно которому оптимальной считается оценка, параметры распределения которой наиболее близки к параметрам распределения истинного вектора состояния изделия.

Заключение.

Анализ ранее разработанного авторами метода оценки технического состояния современных машиностроительных изделий в ходе производственных (приемосдаточных, контрольных) испытаний находится в соответствии с развиваемой в последнее время группой российских ученых теории квалиметрии моделей сложных объектов и может стать основой перспективных программ испытаний. Развитие метода связано с разработкой универсальной методологии испытаний на основе системного подхода к созданию математического обеспечения для интеллектуального организационно-технического комплекса испытаний машиностроительных изделий выделенного класса.

СПИСОК ЛИТЕРАТУРЫ

1. Павленко Е.А. Статистические методы диагностирования технического состояния автомобильных транспортных средств / Е.А. Павленко // Автомобильная промышленность. – 2009. – №7 – С 29 – 30.
2. Халиуллин Ф.Х., Особенности составления диагностической матрицы Байеса при безразборной диагностики двигателей внутреннего сгорания / Халиуллин Ф.Х., Ахметзянов И.Р. // Международный научно-исследовательский журнал, 2016. – № 5 (47).– С. 205-209
3. Макушин А.А. Имитационное моделирование ДВС в рамках автоматизированной системы испытаний / А.А. Макушин, Е.В. Зубков, В.С. Бахвалова // Сборка в машиностроении, приборостроении – №6. – 2009 г. – С. 52 – 56.
4. Pervukhina E. Improvement of the acceptance test procedure for the external combustion engine after assembly by using the relationship between diagnostic parameters / E. Pervukhina, K. Osipov, Y. Rapatskiy // Journal of Machinery Manufacture and Reliability, 2011. – Vol.40. – № 2, – P. 171-175.
6. Охтилев М.Ю. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов / М.Ю. Охтилев, Б.В. Соколов , Р.М. Юсупов. – М.: Наука, 2006, 410 с.
7. Соколов Б.В. Концептуальные основы оценивания и анализа качества моделей и полимодельных комплексов / Б.В. Соколов, Р.М. Юсупов // Теория систем и управления, 2004. – № 6. – С. 5-16.
8. Майданович О.В. Интеллектуальные технологии автоматизированного мониторинга сложных технических объектов / О.В. Майданович // Труды СПИИРАН, 2013. – Вып. 6(29). – Стр. 201-216.
9. МайдановичО.В. Перспективные направления развития информационных технологий мониторинга и управления состояниями сложных технических объектов в реальном масштабе времени / О.В. Майданович, М.Ю. Охтилев, Б.В. Соколов //InternationalJournal "InformationModelsandAnalyses", 2012. – Vol.1. – С.318-335.
10. Епифанов С.В., Выбор эффективных критериев тренда для применения в алгоритмах параметрической диагностики / С.В. Епифанов, Б.А. Щербань, Ю.В. Черкасов // Авиационно-космическая техника и технология, 2012. – № 8 (95). – С. 232-240.
11. Миська А.Р., Трендовый контроль режимных параметров дизель-генераторных установок / А.Р. Миська // Авиационно-космическая техника и технология, 2010. – № 7 (74). – С. 155-158.
12. Emmenegger, J.-F. Harmonic Analysis and Cointegration of Diagnostic Parameter Time Series of Motors / J.-F. Emmenegger, E. Pervukhina, V. Golikova // International Journal of Pure and Applied Mathematics, 2013. – Vol. 82. – №1. –, P. 143-161.
13. Первухина Е.Л. Использование информационной меры в процедурах оценки дискретных стохастических систем при неизвестных ковариациях шумов / Е.Л. Первухина // Известия РАЕН, серия МММИУ, 1999. – т.3. – №3. – С. 100-106.
14. Первухина Е.Л. Управление автоматизированными производственными испытаниями ДВС с использованием информационных технологий / Е.Л. Первухина, В.В. Голикова, К.Н. Осипов, И.С Тимофеев. // «Перспективные системы и задачи управления»: материалы XI Всеросс. научно-практ. конф. и VII молод. школы-семинара «Управление и обработка информации в техн. системах»; ЮФУ. – Ростов-на-Дону : Изд-во ЮФУ, Т. 2. – 2016. – с. 22-30.

УДК 004.492.3

МЕТОДЫ ИЗВЛЕЧЕНИЯ ДАННЫХС ИЗОЛИРОВАННЫХ МАШИН

Романов Александр Алексеевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, ул. Большая Морская, 67
e-mail: R0man0vAleks@yandex.ru

Аннотация. Работа посвящена изучению методов извлечения информации с изолированных машин. Представлены некоторые методы извлечения информации с машин, не имеющих сетевых подключений или какой-либо опасной периферии.

Ключевые слова: *компьютерная безопасность; защита данных; хищение информации; взлом.*

METHODS OF DATA EXTRACTIONFROM ISOLATED MACHINES

Romanov Alexander
St. Petersburg State University of Aerospace Instrumentation
Russia, St. Petersburg, Bolshaya Morskaya str., 67
e-mail: R0man0vAleks@yandex.ru

Abstract. The paper is dedicated to studying of methods of extract information from isolated machines. Some methods of extract information from machines without network connection or any dangerous peripherals are shown in the article.

Keywords: *computer security; data protection; theft of information; hacking.*

В современном мире информация стала важнейшим ресурсом во всех отраслях нашей жизни. Именно по этой причине мы стараемся защитить её всеми возможными средствами. Распространено мнение, что основной угрозой для данных, хранящихся на компьютерах, является подключение к сети или использование потенциально опасной периферии. В работерассматриваются методы извлечения информации с изолированных машин, то есть таких машин, которые не имеют сетевых подключений или какой-либо опасной периферии.

Одним из таких методов является передача данных с помощью мигания индикатора использования жёсткого диска. Такие индикаторы присутствуют в большинстве персональных компьютеров и ноутбуков. Данные светодиоды обладают возможностью мерцания с частотой 6000 раз в секунду, а передавать информацию можно, используя двоичный код, где горящий светодиод обозначает 1, а потухший - 0.

Другим методом может быть использование подключенных наушников в качестве микрофона. Как известно, на аппаратном уровне микрофон и наушники не сильно отличаются друг от друга. Этот факт даёт возможность использовать наушники для улавливания колебаний воздуха в радиусе примерно 6 метров от заражённой машины, а запись можно осуществить, обратив выходной канал звуковой карты во входной.

Ещё одним способом извлечения информации является использование USB девайса в качестве RF-трансмиттера. Для применения этого метода подойдёт практически любая флешка, при этом нет необходимости каким-либо образом её модифицировать. Чтобы начать передачу данных, достаточно отправить на USB устройство последовательность нулей, это создаст электромагнитное излучение в диапазоне от 240 до 480 МГц. Управляя данным процессом, можно научить ресивер воспринимать излучение как поток нулей и единиц. Таким образом, можно получить возможность передавать информацию на расстояние до трёх метров, если устройство имеет провод, который может быть использован как антенна, можно увеличить расстояние передачи до восьми метров.

В качестве ещё одного метода можно применить прослушивание звуков работы жёсткого диска. SSD для данного метода не подойдут, так как не имеют движущихся частей, а шум HDD и SSHD с помощью программы, управляющей позиционером диска, можно использовать для передачи данных. В качестве приёмника подойдёт любое устройство, оснащённое микрофоном и расположенное вблизи корпуса заражённой машины.

Также для извлечения информации можно использовать электромагнитное излучение видеокарты, которое воспринимается FM приёмником мобильного телефона. Этот метод позволяет использовать обычный мобильный телефон для распознавания сигнала видеокарты заражённого компьютера. С помощью данной технологии исследователям удалось получить информацию с расстояния до семи метров.

В работе представлены лишь некоторые из способов, которыми могут воспользоваться злоумышленники для хищения данных, однако, все они требуют, чтобы машина изначально была заражена вредоносной программой, что уже, вероятно, является непростой задачей. В качестве основных способов обеспечения безопасности можно назвать необходимость лучше контролировать область в непосредственной близости от вероятного объекта интереса злоумышленников и запрет на использование каких-либо устройств, подверженных модификациям в одном помещении с данной машиной. Также, вероятно, стоит ограничить обзор со стороны на рабочее место и подумать об экранировании стен в помещении.

СПИСОК ЛИТЕРАТУРЫ

1. Mordechai Guri, Boris Zadov, Eran Atias,Yuval Elovici. LED-it-GO Leaking (a lot of) Data from Air-Gapped Computers via the (small) Hard Drive LED. Ben-Gurion University of the Negev. Cyber Security Research Center.
2. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. SPEAKE(a)R: Turn Speakers to Microphones for Fun and Profit. Ben-Gurion University of the Negev. Cyber Security Research Center.
3. Mordechai Guri, Matan Monitz, Yuval Elovici. USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB. Ben-Gurion University of the Negev. Cyber Security Research Center.
4. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise. Ben-Gurion University of the Negev. Cyber Security Research Center.
5. How to leak sensitive data from an isolated computer (air-gap) to a near by mobile phone - AirHopper. URL: http://cyber.bgu.ac.il/content/how-leak-sensitive-data-isolated-computer-air-gap-near-mobile-phone-airhopper.

УДК 004

БЛОКЧЕЙН-ТЕХНОЛОГИИ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ УПРАВЛЕНИИ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИМИ СИСТЕМАМИ

Токарев Алексей Игоревич
Севастопольский государственный университет
Россия, Севастополь, ул. Университетская, 33
e-mail: tokalig@mail.ru

Аннотация. Рассмотрены основные задачи поддержки принятия решений при управлении социально-экономическими системами в условиях инновационного развития отечественной экономики, в том числе с целью обеспечения информационной безопасности.

Ключевые слова: *инновационное развитие; принятие решений; распределенное хранилище данных; блокчейн.*

BLOCKCHAIN-TECHNOLOGIES PROVIDINGINFORMATION SECURITY AT THEDECISION MAKING TO CONTROL THE SOCIO-ECONOMIC SYSTEMS

Tokarev Aleksey
Sevastopol's State University
Russia, Sevastopol, Universitetskaya str., 33
e-mail: tokalig@mail.ru

Abstract. The main problems of the decision making to control social and economic systems under the conditions of innovative development of national economy are considered, as well as to providean information security.

Keywords: *innovative development; decision-making; distributed data storage, blockchain.*

Инновационное развитие отечественной экономики подразумевает соблюдение ряда условий: проведения кадровой политики через механизмы конкуренции и отбора руководящих кадров, участия экспертовдля эффективного управления социально-экономическими системами, в том числе, создающих, внедряющих и активно использующих современные технологии принятия управляющих решений [1].

При управлении социально-экономической системой поддержка принятия решений заключается в выборе оптимальной стратегии ее функционирования и развития. Необходимые для этого алгоритмы и информационные технологии создаются на основе преобразования содержательных целей ее управления в формальные показатели и критерии, а также оперативного моделирования и анализа текущих данных, получаемых одновременно из различных источников.

Обеспечение независимости отечественной экономики при этом требует решения вопроса об информационной безопасности системы управления. Потеря данных или их замена может привести к ошибочным управленческим решениям и, как следствие, неблагоприятным последствиям для экономики. Поэтому одной из важных задач является обеспечение безопасности хранения и передачи данных. Внедрение блокчейн технологий является одним из современных средств замены существующих серверов с возможностью таких функций. Блокчейн – вид распределенной базы данных, представляющей цепь связанных блоков данных. В каждом из блоков есть ссылка на предыдущий блок.

Таким образом, невозможно изменить данные в существующих блоках, а транзакции в новом блоке, прикрепляемом к цепи, содержат вводную информацию из предыдущих блоков [2]. В системе поддержки принятия решений данная технология может использоваться для хранения любых данных, представляющих какую-либо ценность. Количество данных, хранимых в блокчейне, не ограничено, но эффективность использования технологии зависит от вычислительных мощностей узлов. Любое действие, записываемое в блокчейн, остается в нем навсегда, эту информацию нельзя удалить и изменить, следовательно, с каждой транзакцией растет объем хранимых данных. Все данные доступны и открыты для всех участников, применен транзакционный подход к хранению данных, который позволяет получить информацию об изменениях каждого элемента данных и все прошлые версии любого элемента.Возможно разграничение доступа к данным путем использования криптографической защиты.Значительным преимуществом решения является распределение данных между всеми узлами системы, что делает практически невозможным замену, похищение и удаление данных, а, следовательно, исключенавероятность принятия неверного управленческого решения по причине некорректности или отсутствия уже сохраненных программой данных.

СПИСОК ЛИТЕРАТУРЫ

1. Окулич-Казарин В.П., Голобородько А.Ю. Четыре условия инновационного развития экономики России. - Warszawa: Wydawca: Sp. z o.o. «Diamondtradingtour», 2015, 11 с.
2. ПряниковМ.М., Чугунов А.В.Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы– InternationalJournalofopenInformationTechnologies, 2017, 49 с.

УДК 004

КОМПЛЕКСНАЯ СИСТЕМА ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ КАБИНЕТА РУКОВОДИТЕЛЯ. ЭФФЕКТИВНОСТЬ РАБОТЫ ПРИБОРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ КОМПЛЕКСНОЙ СИСТЕМЫ ИНЖЕНЕРНО ТЕХНИЧЕСКОЙ ЗАЩИТЫ КАБИНЕТА РУКОВОДИТЕЛЯ

Фаязов Кобилджон Абдукаюмович
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mail: kobil93@mail.ru

Аннотация. В статье рассмотрены системы защиты информации, также эффективность используемых приборов, различные вопросы инженерно-технической защиты информации также предпринята попытка систематизировать большой объем часто противоречивых сведений по инженерно-технической защите информации.

Ключевые слова: *защита кабинета; руководитель; защита информации; средства защиты.*

INTEGRATED SYSTEM OF ENGINEERING AND TECHNICAL PROTECTION OF THE MANAGER'S OFFICE. THE EFFECTIVENESS OF THE WORK OF INFORMATION SECURITY DEVICES ON THE EXAMPLE OF AN INTEGRATED SYSTEM OF ENGINEERING AND TECHNICAL PROTECTION OF THE MANAGER'S OFFICE

Fayazov Kobiljon
University of ITMO
Russia, St. Petersburg, Kronverkskiy pr., 49
e-mail: kobil93@mail.ru

Abstract. The article considers information security systems, also the efficiency of the devices used, various issues of engineering and technical protection of information, an attempt is also made to systematize a large volume of often contradictory information on engineering and technical protection of information.

Keywords: *protection of the cabinet; leader; data protection; protection devices.*

Введение. Защита информации представляет собой многоцелевую проблему, часть которой еще даже не имеет четкой постановки. Наиболее разработаны вопросы защиты информации, содержащей государственную, коммерческую и прочие тайны.

Система защиты информации, обрабатываемой с использованием технических средств, должна строиться по определенным принципам. Это обусловлено необходимостью противодействия целому ряду угроз безопасности информации.

Основным принципом противодействия угрозам безопасности информации, является превентивность принимаемых мер защиты, так как устранение последствий проявления угроз требует значительных финансовых, временных и материальных затрат.

Принцип системного подхода к построению системы противодействия угрозам безопасности позволяет заложить комплекс мероприятий по защите информации уже на стадии проектирования, обеспечив оптимальное сочетание организационных и технических мер защиты информации. Важность реализации этого принципа основана на том, что дополнение функционирующей незащищенной автоматизированной системы средствами защиты информации сложнее и дороже, чем изначальное проектирование и построение защищенной системы.

Необходимо отметить, что актуальность и значимость проблем, касающихся обеспечения информационной безопасности государства, личности и общества в нашей стране, давно вывели их за узкотехнические рамки, придав им общественно-политическую значимость. Динамично развивается тенденция расширения круга лиц, интересующихся вопросами защиты информации, как важного компонента обеспечения их законных прав и демократических свобод.

Рассмотрению различных вопросов инженерно-технической защиты информации посвящен данный дипломный проект. Здесь предпринята попытка систематизировать большой объем часто противоречивых сведений по инженерно-технической защите информации.

Особенностью методических основ инженерно-технической защиты информации является то, что в них рекомендуется объединить практические и лабораторные работы единым сценарием решения сложной практической задачи по защите информации. В качестве примера такого сценария в дипломе рассматриваются методические вопросы защиты информации в одном из наиболее сложных объектов — кабинете руководителя организации.

Технические средства противодействия наблюдению

Основными средствами скрытия объектов наблюдения в оптическом диапазоне являются краски, различные маски и экраны. При выборе красок для маскировочного окрашивания кроме цвета важно учитывать характер изменения коэффициента отражения от длины волны. Чем меньше

отличаются коэффициенты отражения краски в видимом и инфракрасном диапазонах волн, тем лучше ее маскирующая способность.

Искусственные оптические маскировочные маски в зависимости ее формы и способа расположения возле объекта делятся на следующие типы:

- маски-навесы;
- вертикальные маски;
- маски перекрытия;
- наклонные маски;
- радиопрозрачные маски.

Маски-навесы предназначены для скрытия объектов, расположенных на открытых сверху площадках и защищают их от наблюдения с помощью средств, размещаемых на верхних этажах высотных зданий, возвышенностях и горах, на самолетах и космических аппаратах.

Вертикальные маски защищают объекты от наблюдения с земли. Маски перекрытия состоят из каркаса и маскировочного покрытия, которые полностью закрывают объект. Они применяются, прежде всего, для защиты объектов, перевозимых на открытых платформах.

Наклонные маски используются в основном для скрытия теней объемных объектов, по длине которых с учетом положения солнца определяют высоту объектов при наблюдении сверху (с самолетов и космических аппаратов).

Радиопрозрачные маски выполняются из радиопрозрачных материалов (стеклопластика, пенопласта и др.), обычно в форме шара, для скрытия демаскирующих признаков и физической защиты антенн.

Для дезинформирующего скрытия применяются кроме деформирующих масок ложные сооружения и конструкции, создающие признаки ложного объекта (объекта прикрытия). Ложные сооружения могут быть плоскими и объемными, функциональными и нефункциональными. Они относятся к наиболее дорогим средствам защиты информации, особенно объемные и функциональные, так как должны воспроизводить полный набор демаскирующих признаков объекта прикрытия в динамике в течение всего периода защиты. Если, например, имитируется объект, на котором работают люди, то они должны убедительно изображать соответствующую деятельность, а не устраивать непрерывные перекуры или греться на солнышке.

Энергетическое скрытие демаскирующих признаков объектов достигается путем уменьшения яркости объекта и фона ниже чувствительности глаза или технического фотоприемника, а также их ослепления. Наиболее естественным способом энергетического скрытия является проведение мероприятий, требующих защиты информации о них, ночью. Яркость объектов, имеющих искусственные источники света, снижается путем их выключения или экранирования светонепроницаемыми шторами и экранами.

Для экранирования объектов наблюдения в помещении применяются шторы, занавески, жалюзи, тонированные стекла и пленки. Эффективные экраны создают жалюзи. По виду материалов жалюзи делятся на тканевые, пластиковые, деревянные и металлические. Лучшие эксплуатационные свойства имеют деревянные и металлические жалюзи. По расположению ламелей жалюзи бывают вертикальные, горизонтальные и рулонные.

Технические средства предотвращения утечки информации с помощью закладных подслушивающих устройств

Классификация технических средств обнаружения и локализации закладных устройств приведена на рисунке 1.

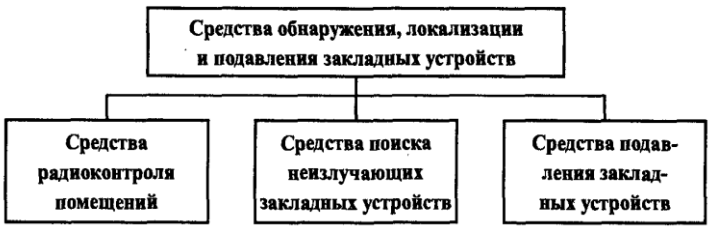


Рисунок 1. Классификация средств обнаружения и локализации закладных устройств.

Средства радиоконтроля помещения предназначены для обнаружения закладных устройств, излучающих радиоволны во время их поиска. Для обнаружения не излучающих при поиске закладок — дистанционно управляемых и передающих сигналы по проводам применяются средства, реагирующие не на радиоизлучения, а на иные демаскирующие признаки закладок. Наконец, средства подавления закладных устройств обеспечивают энергетическое скрытие их сигналов, нарушение работоспособности закладок или их физическое разрушение.

Информационно-техническое сопряжение сканирующих приемников с переносными компьютерами послужило технической основой для создания автоматизированных комплексов для быстрого и надежного поиска радиоизлучающих подслушивающих устройств.

Обнаружитель поля представляет собой широкополосный приемник прямого усиления (в простейшем случае— детекторный) с телескопической штыревой антенной. Усиленные сигналы, превышающие по уровню вручную устанавливаемое пороговое значение, подаются на световой и звуковой индикаторы, информирующие оператора о наличии в месте нахождения антенны электромагнитного поля с мощностью, превышающей пороговое значение. Перед поиском закладки индикатор поля настраивается на уровень фона в обследуемом помещении. С этой целью оператор, находясь в точке помещения на удалении нескольких метров от возможных мест размещения закладок, устанавливает регулятор чувствительности в такое положение, при котором индикатор находится на грани срабатывания. При приближении индикатора поля к излучающей закладке напряженность электромагнитного поля возрастает, повышается уровень сигнала в антенне и, соответственно, на входе индикатора поля. При превышении уровня порогового значения, определяемого положением регулятора чувствительности, индикатор срабатывает, оповещая о появлении в обследуемой зоне электромагнитного поля мощностью, превышающей мощность фона. С целью большей информативности световых индикаторов их выполняют в современных обнаружителях поля в виде линейки из 4-10 светодиодов. Каждый последующий светодиод излучает свет при повышении уровня электромагнитного поля.

Комплекс при минимальном участии оператора определяет и запоминает уровни и частоты радиосигналов в контролируемом помещении, выявляет в результате корреляционной обработки спектрограмм вновь появившиеся излучения, с использованием тестового акустического сигнала распознает скрытно установленные в помещении радиомикрофоны и определяет их координаты. Возможности комплексов расширяют также включением в их состав блока контроля проводных линий, позволяющего обнаруживать подслушивающие устройства, подключенные к проводам кабелей.

В комплект современных автоматизированных комплексов радиомониторинга включают генератор прицельных помех. Он обеспечивает возможность оперативно настраиваться на частоту обнаруженного закладного устройства и подавлять его сигналы в условиях, когда нет времени на поиск и нейтрализацию закладного устройства, например, во время совещания.

С целью сокращения времени просмотра диапазона частот до нескольких минут анализ сигналов в перспективных комплексах проводится на основе быстрого преобразования Фурье.

Создание и применение автоматизированных комплексов для непрерывного радиомониторинга помещений с конфиденциальной информацией является наиболее эффективным направлением развития средств для комплексной защиты информации от утечки по радиоэлектронному каналу.

Средства контроля телефонных линий и цепей электропитания.

Учитывая повсеместное распространение телефонов как средств коммуникаций и повышенный интерес злоумышленников к подслушиванию телефонных разговоров, большое внимание при обеспечении защиты информации уделяется способам и средствам контроля телефонных линий.

Способы контроля телефонных линий основаны на том, что любое подключение к ним вызывает изменение электрических параметров линий и сигналов в них: напряжения и тока в линии, значений емкости и индуктивности линии, активного и реактивного ее сопротивлений. В зависимости от способа подключения подслушивающего устройства к телефонной линии (последовательного — в разрыв провода телефонного кабеля или параллельного) влияние подключаемого подслушивающего устройства может существенно отличаться. Так как закладное устройство использует энергию телефонной линии, величина отбора мощности закладкой из телефонной линии зависит от мощности передатчика закладки и его коэффициента полезного действия.

Для контроля телефонных линий применяются следующие устройства:

– устройства оповещения световым и звуковым сигналом об уменьшении напряжения в телефонной линии, вызванном несанкционированным подключением средств подслушивания к телефонной линии;

– измерители параметров телефонных линий (напряжения, тока, емкостного сопротивления, волнового сопротивления и др.), при отклонении которых от номинального значения формируется сигнал тревоги;

– «кабельные радары», позволяющие выявлять неоднородности телефонной линии и измерять расстояние до неоднородности (асимметрии постоянному току в местах подключения подслушивающих устройств, обрыва, короткого замыкания и др.)

Технические средства предотвращения утечки информации с помощью закладных подслушивающих устройств.

Одной из наиболее сложных задач в области защиты информации является поиск внедренных ЗУ, не использующих радиоканал для передачи информации, а также радиозакладок, находящихся в пассивном (неизлучающем) состоянии. Традиционные средства выявления такие, как панорамные радиоприемники, анализаторы спектра или детекторы поля, в этом случае оказываются неэффективны. Визуальный осмотр также не гарантирует обнаружение подобных ЗУ, так как современные технологии позволяют изготовлять их с любым видом камуфляжа, прятать в элементах строительных конструкций и интерьера. Именно эта проблема и привела к появлению совершенно нового вида поискового прибора, получившего название нелинейного радиолокатора. Это, пожалуй,

наиболее уважаемый вид поисковой техники (жаль, что в силу высокой цены не наиболее покупаемый!). Обусловлено это его уникальной способностью обнаруживать любые радиоэлектронные устройства в строительных конструкциях, предметах интерьера и т.д., что делает нелинейные локаторы абсолютно незаменимыми при проведении поисковых мероприятий. Именно к нелинейным локаторам по праву можно отнести утверждение, что российская спецтехника по цене значительно ниже, а по качеству выше, чем зарубежные аналоги.

Профессиональный нелинейный локатор "NR-900V"

Преимущества:

– возможность работы в сложных помеховых условиях, высокая результативность поиска при обследовании капитальных строительных конструкций, режим «идентификация» снижает вероятность ложных обнаружений;

– дополнительный индикатор уровней сигнала, расположенный на антенной системе;

– продолжительное время непрерывной работы без замены источника питания.

Нелинейный локатор "NR-T"

Предназначен для поиска электронных средств связи (СИМ-карт, миниатюрных средств звукозаписи, сотовых телефонов, радиостанций) в местах, где пользование ими запрещено (СИЗО, места лишения свободы) а также для выявления средств связи (сотовых телефонов, радиостанций) и других радиоэлектронных устройств независимо от их функционального состояния «включено/выключено», в сторожевом или ждущем режиме.

Преимущества:

– эффективно обнаруживает малоразмерные цели (СИМ-карты, миниатюрные злектронные устройства)

– повышенная помехоустойчивость к откликам от строительных конструкций и элементов интерьера (контакты МОМ)

– дополнительно усиленные разъемные соединения, дополнительные меры по защите от влаги и коррозии для сложных условий эксплуатации

– облегченная батарея повышенной емкости, встроенная в блок приемопередатчика, продолжительное время непрерывной работы без замены источника питания

– специальный подсумок для размещения аппаратуры на теле оператора

Детектор скрытых видеокамер "WCH-900"

WCH-900 представляет собой детектор камер, передающих изображение в диапазоне от 900 МГц до 2700 МГц. Указанный диапазон является стандартным для радиоканальных камер.

Детектор скрытых камер WCH-900 способен принимать сигнал радиоканальных видеокамер, что позволяет просматривать их изображение, а также локализовывать их место нахождения. Видео-сканер автоматически сканирует заданный диапазон частот и определяет модуляцию, что позволяет детектору скрытых камер WCH-900 в автоматическом режиме просматривать изображение радиоканальной видеокамеры. Этот прибор обеспечит полную безопасность Ваших встреч или переговоров!

Особенности детектора скрытых камер WCH-900:

WCH-900 способен автоматически определять протокол передаваемого сигнала.

Видео-сканер имеет автоматический и ручной режимы настройки прибора.

Дальность обнаружения равняется дальности передатчика.

Детектор камер имеет возможность прослушивания акустического сигнала.

На экране прибора отражена следующая информация: чувствительность антенны, частоты сканирования, заряд АКБ.

Питание WCH-900 происходит от 4 батарей AA или от сетевого адаптера.

В видео-сканере имеется возможность скоростного сканирования диапазона 900–2700 МГц.

Автоматизированные поисковые комплексы

Для обнаружения, поиска и нейтрализации подслушивающих устройств в последнее время все более широко используются автоматизированные поисковые комплексы. В простейшем случае такие комплексы состоят из стандартного сканирующего приемника, управляющей ПЭВМ и специального программного обеспечения. Наиболее известные на российском рынке системы такого рода комплекс RS1000 и комплексы, построенные на базе ПО SEDIF.

Более сложные комплексы помимо сканирующего приемника (чаще всего модернизированного) имеют в составе ряд дополнительных устройств, расширяющих их функциональные возможности (устройства для проверки проводных коммуникаций, постановщики помех, блоки БПФ и т.п.). В качестве примера таких устройств можно привести семейство комплексов АРК, ДЕЛЬТА, КРОНА. К сожалению, стоит отметить, что цена таких комплексов увеличивается прямо пропорционально количеству используемых в них дополнительных устройств.

В настоящее время наибольший интерес вызывают многофункциональные комплексы типа RS1100 и АРК-Д3, построенные по модульной схеме, на базе которых можно создавать

многоканальные системы (до 24 каналов) для одновременного контроля нескольких пространственно разнесенных помещений или всего здания.

Цифровой Зонд/монитор "СРМ-700" (Акула)

СРМ-700 — универсальный прибор для обнаружения основных типов электронных устройств негласного съема информации, включая комнатные, телефонные, носимые на теле "жучки" , видеопередатчики и звукозаписывающие устройства.

Многофункциональный поисковый прибор ST 032

Предназначен для проведения мероприятий по обнаружению и локализации специальных технических средств негласного получения информации, для выявления естественных и искусственно созданных каналов утечки информации, а также для контроля качества защиты информации.

Представляет собой модификацию модели ST 031 "ПИРАНЬЯ".

Отличается компактным исполнением и простотой эксплуатации.

СПИСОК ЛИТЕРАТУРЫ

1. Торокин А. А. Инженерно-техническая защита информации. — М.: Гелиос АРВ, 2005.
2. Хорев А. А. Способы и средства защиты информации.— М.: МО РФ, 1998.
3. Волокитин А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Информационная безопасность государственныхорганизаций и коммерческих фирм. - Справочное пособие (под общейредакцией Реймана Л.Д.) М: НТЦ «ФИОРД-ИНФО», 2002г.-272с.
4. Бюро научно-технической информации, http://www.bnti.ru/
5. Защита информации, http://www.sinf.ru/index.htm

УДК 004.942

ПРИМЕНЕНИЕ ДИНАМИЧЕСКОЙ МОДЕЛИ ПРОТИВОБОРСТВА ДЛЯ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННЫХ СИСТЕМ

Шишкин Владимир Михайлович[1], Колесников Константин Евгеньевич[2]
[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург,14 линия, 39
[2]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Россия, Санкт-Петербург, ул. Профессора Попова, 5
e-mails: vms@iias.spb.su, yakoston@gmail.com

Аннотация.Рассматривается дифференциальная макромодель противоборства, как инструмент для принятия решений при обеспечении безопасности информационных систем в агрессивном окружении. Приводятся результаты проведённых на модели вычислительных экспериментов.

Ключевые слова: *макромоделирование; противоборство; управление; дифференциальные уравнения; вычислительный эксперимент.*

APPLICATION OF DYNAMIC MODEL OF CONFRONTATION FOR MANAGEMENT OF INFORMATION SYSTEMS SECURITY

Shishkin Vladimir[1], Kolesnikov Konstantin[2]
[1]St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences
14-th Linia, V.O., 39, St. Petersburg, Russia
[2]St. Petersburg Electrotechnical University "LETI"
Professora Popovastr.,5 St. Petersburg, Russian Federation
e-mails: vms@iias.spb.su, yakoston@gmail.com

Abstract. The differential macromodel of confrontation is considered like a tool for decision-making for ensuring security of the information systems in an aggressive environment. Results of the made on model are given.

Keywords: *macromodeling; confrontation; management; differential equations;* computing experiment.

Современный этап развития общества и технологий характеризуется противоречивостью и усилением конфликтности отношений субъектов. Обеспечение безопасности становится невозможным без активного противодействия, превращаясь в противоборство.

Для описания динамики противоборства была построена дифференциальная модель [1], основанная на более раннем исследовании взаимодействия развития информационно-коммуникационных технологий и национальной безопасности [2, 3]. Опыт применения подобного рода сравнительно простых динамических моделей в различных предметных областях, в том числе плохо формализуемых, имеет уже давнюю историю.

В процессе развития модели сложились более универсальные формулировки и определения, и оказалось, что модель масштабируема, и без изменения её структуры, вложив несколько иной содержательный смысл в некоторые фазовые переменные, её можно интерпретировать в широком диапазоне от межгосударственного взаимодействия до, например, внутрикорпоративного уровня или даже технических процессов взаимодействия.

Определено, что любая моделируемая система как минимум выполняет три основных функции: «Основная деятельность системы», «Обеспечивающая деятельность системы» и «Система обеспечения безопасности».

С целью оценки безопасности информационных систем (ИС), предназначенных для обработки и хранения информации, данная модель была интерпретирована в соответствующих терминах. Кроме этого, модель начала носить прикладной характер, и стороны противоборства уже рассматриваются как «Своя система» и «Система противника» (ранее эти стороны имели абстрактный характер). Так основные фазовые переменные теперь имеют следующие наименования (приведенный ниже перечень не исчерпывающий):

Для «Своей системы»:

Основная деятельность системы – обработка и хранение информации (понимается вместе с передачей информации по каналам связи);

Обеспечивающая деятельность системы – организационная и модернизационная деятельность компании (техническая поддержка системы и работы по её усовершенствованию);

Система обеспечения безопасности – аппаратно-программное и организационно-правовое обеспечение безопасности (уровень оценивается по соответствию требованиям международным и государственным стандартам и выполнению мероприятий сверх указанных норм);

Стоит добавить, что термины ресурс, уровень угроз и уровень безопасности не изменились.

Система противника может иметь разнообразные реализации, но структурно по определению она имеет такие же блоки.

Основная деятельность системы – нанесение вреда ИС (под это определение попадают и DDoS-атаки, и вирусное заражение, и промышленный шпионаж и т.п.);

Обеспечивающая деятельность системы – изучение и применение новых технологий;

Уровень безопасности – живучесть (для злоумышленников важно, чтобы их деятельность продолжалась максимально-возможное время. На это влияет анонимность, квалификация, результаты атак и т.д.);

Уровень угроз прямо зависит от способности атакуемой системы противодействовать угрозам.

Что касается ресурса атакующей системы, то это, прежде всего мотивация и финансирование. Причем, мотивация сильнее влияет на злоумышленника, а финансирование может выступать как мотивирующий фактор.

Теперь, когда формально определены стороны, можно задать параметры дифференциальной модели противоборства и решать задачи обеспечения безопасности информационной системы.

В ходе экспериментов была выявлена прямая зависимость уровня безопасности информационной системы и её способности к выживанию в агрессивной среде. Отсюда следует вывод, что для поддержки жизнеспособности системы необходимо уделять особое внимание и выделять ресурсы для обеспечения безопасности. Угнаться за темпом появления средств защиты информации сложно, да и уделяя внимание только защите можно пропустить момент, когда деятельность системы станет попросту неактуальной.

Поэтому важно четко расходовать и рациональнораспределять свои ресурсы. Эксперименты показали правдоподобность поведения модели.

Основное влияние на систему в сети оказывают вирусные эпидемии и хакерские атаки. Их сложно предугадать, но при достаточном количестве ресурса и специальной подготовке можно не только обнаруживать, но и предотвращать негативные воздействия на систему.

Но стоит понимать, что защита информационной системы не заканчивается на периметре сети. Атака начинается с разведки, и порой, злоумышленники применяют методы социальной инженерии, чтобы получить необходимую информацию, а иногда, и нанести вред системе изнутри. Эти и другие факторы также можно учесть в составе фазовых переменных.

В докладе представлены структурная схема дифференциальной модели, интерпретированная в соответствующих терминах, математическая модель, результаты проведенных экспериментов и перспективы развития модели.

Заключение.

Как только появляется злоумышленник, противник, ИС явно или не явно вступает с ним в противоборство. В процессе противоборства расходуется большое количество ресурса, и ошибка может стоить дорого. Поэтому для подготовки принятия решений, предлагается использовать дифференциальную модель, позволяющую прогнозировать потенциальную динамику взаимодействия сторон, что позволит своевременно формировать упреждающие воздействия.

СПИСОК ЛИТЕРАТУРЫ

1. Колесников К.Е., Шишкин В.М. Исследование динамики симметричного противоборства на дифференциальной модели // Информационная безопасность социально-экономических систем: монография / Апатова Н.В. и др. / под ред. проф. О.В. Бойченко. – Симферополь: ИП Зуева Т.В., 2017. – 348 с.
2. Шишкин В.М., Абросимов И.К. Динамическая модель системы взаимодействия развития ИКТ и обеспечения национальной безопасности // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. — СПб.: 2015. — С. 230-235.
3. Юсупов Р.М., Шишкин В.М. Информационно-коммуникационные технологии и национальная безопасность – противоречивая реальность // Информатизация и связь, № 1, 2010. – С. 27-35.

УДК 004.056

МОДЕЛЬ ОБНАРУЖЕНИЯ ВНУТРЕННИХ НАРУШИТЕЛЕЙ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ БОЛЬШИХ ДАННЫХ

Ушаков Игорь Александрович[1], Котенко Игорь Витальевич[2]
[1]Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича, Россия, Санкт-Петербург, пр. Большевиков, 22, корп. 1
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mails: ushakovia@gmail.com, ivkote@comsec.spb.ru

Аннотация. В работе представлена модель обнаружения внутренних нарушителей безопасности с использованием технологий больших данных. В настоящее время наблюдается огромный рост сетевого корпоративного трафика, прежде всего за счет использования пользователями мобильных устройств. В связи с этим крайне актуальной становится задача обеспечения своевременного выявления нарушителей безопасности корпоративной сети с использованием технологий больших данных.

Ключевые слова: *большие данные; информационная безопасность; моделирование; внутренний нарушитель.*

MODEL OF DISCOVERY AN INSIDE ATTACKER BASED ON BIG DATA TECHNOLOGIES

UshakovIgor[1], Kotenko Igor[2]
[1] Bonch-Bruevich St. Petersburg State University of Telecommunications
Russia, St. Petersburg, Bolshevikov pr., 22
[2] St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya,39
e-mails: ushakovia@gmail.com, ivkote@comsec.spb.ru

Abstract. This article presents a model of discovery an inside attackers based on Big Data technologies. Nowadays there is a huge amount of network corporate traffic, first of all because corporate users more often use mobile devices. In this regard, it is becoming extremely urgent task to ensure timely detection of corporate network security attackers using Big Data technologies.

Keywords: *Big Data; information security; modeling, inside attacker.*

Век информационных технологий сопровождается непрерывным ростом интернет трафика. В частности, рост мобильного трафика в 2016 году составил 46% и достиг 7,2 экзабайтов в месяц [1]. Экспоненциальный рост объема трафика связан с массовым распространением и удешевлением мобильных цифровых устройств и услуг связи, проникновением Интернета в повседневную жизнь. Так количество мобильных устройств увеличилось в 50 раз по сравнению с 2003 годом, на каждого жителя Земли приходится 3.47 таких устройств [1].

В связи с расширением возможных вариантов подключения и большого разнообразия пользовательских устройств появляются новые риски нарушения безопасности. Для обеспечения информационной безопасности корпоративной ИТ-инфраструктуры требуется обеспечить сбор подробных сведений обо всех сетевых взаимодействиях в сети организации. Для этой цели целесообразно применить технологии больших данных [2,3] в совокупности с известными средствами обеспечения информационной безопасности корпоративной среды.

В работе подробно рассматриваются основные методы обнаружения внутренних нарушителей безопасности корпоративной ИТ-инфраструктуры, включая такие методы как профилирование, контроль доступа, управление гостевым доступом, оценка состояния оконечных устройств, сервис защиты оконечных устройств, мониторинг пользователей.

Работа выполнена при финансовой поддержке РФФИ (проекты 15-07-07451, 16-29-09482 офи_м) и бюджетных тем № 0073-2015-0004.

СПИСОК ЛИТЕРАТУРЫ

1. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper

2. Котенко И.В., Ушаков И.А. Технологии больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд. 2017. № 3 (75). С. 23-33.
3. Котенко И.В., Ушаков И.А. Использование технологий больших данных для мониторинга инцидентов информационной безопасности // XV Санкт-Петербургская Международная Конференция “Региональная информатика-2016” (“РИ-2016”). Материалы конференции. СПб., 2016. С.168-169.

УДК 004.056

БАЗЫ ДАННЫХ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ: ПРИМЕНЕНИЕ SQL И NOSQL ТЕХНОЛОГИЙ

Ушаков Игорь Александрович[1], Котенко Игорь Витальевич[2]
[1]Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича, Россия, Санкт-Петербург, пр. Большевиков, 22, корп. 1
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mails: ushakovia@gmail.com, ivkote@comsec.spb.ru

Аннотация. Работа направлена на решение задач построения баз данных безопасности компьютерной сети с использованием баз данных SQL и NoSQL. В докладе представлен сравнительный анализ SQLи NOSQLтехнологий построения баз данных, делается вывод о целесообразности NoSQL-подхода.

Ключевые слова: *большие данные; информационная безопасность; моделирование; SQL-базы данных; NoSQL-базы данных.*

SECURITY DATABASES FORA CORPORATIVE NETWORK: IMPLEMENTING SQL AND NoSQL TECHNOLOGIES

Ushakov Igor[1], Kotenko Igor[2]
[1]Bonch-Bruevich St. Petersburg State University of Telecommunications
Russia, St. Petersburg, Bolshevikovpr., 22
[2] St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
e-mails: ushakovia@gmail.com, ivkote@comsec.spb.ru

Abstract. This work is about solving tasks of design of a computer network security data base using SQL and NoSQL technologies. The report presents the comparative analysis of SQL and NOSQL technologies of building data bases, making conclusion about usability of NoSQL data bases.

Keywords: *Big Data; information security; modeling; SQL-data bases; NOSQL-data bases.*

Стремительный рост количества Интернет-трафика за последнее десятилетие, вызванного появлением мобильных устройств и развитием новых высоконагруженных платформ и социальных сетей с многомиллионной аудиторией пользователей привел к появлению термина Big Data (“Большие данные”). Данный термин объединяет в себе различные подходы, способы и средства распределенной обработки разнородной информации огромных объемов [1].

С появлением инструментов для разработки систем (таких, как Apache Hadoop, Spark), использующих концепцию больших данных, встает вопрос об использовании технологий больших данных для информационной безопасности и, в частности, систем мониторинга безопасности [2-4].

Количество трафика продолжает расти из года в год, и становится все сложнее обнаруживать потенциальные угрозы безопасности. Пропускная способность современных систем мониторинга и предупреждения сетевых атак перестает удовлетворять требованиям постоянно разрастающихся сетей: в связи с большим количеством поступающего трафика и низкой скоростью его обработки результаты такого анализа получаются неактуальными и не отражают реального состояния сети [5].

Для решения задач хранения огромных объемов трафика были предложены различные средства. Одно из них - проект с открытым исходным кодом Hadoop [6]. Подробная структура Hadoop была представлена авторами в работе [7].

Hadoop предоставляет возможность хранить данные в базе данных.

Выделим три основных требования к базам данных безопасности:

1. Консистентность- это свойство подразумевает сохранение целостности данных после выполнения каких-либо операций. Например, после обновления данных все клиенты базы данных увидят одинаковые данные.

2. Доступность-свойство системы работать бесперебойно.

3. Устойчивость к разделению-это свойство гарантирует работоспособность базы данных даже при нарушении коммуникаций между отдельными узлами кластера.

Теоретически достигнуть всех трех требований невозможно. Традиционные SQL-базы данных входят представляют собой нераспределенный кластер, в котором все узлы связаны между собой. При нарушении связности кластера нарушается и работоспособность базы данных. NoSQL-базы данных обеспечивают консистентность данных ценой их доступности или, наоборот, доступность в ущерб консистентности.

Ввиду распределенности и необходимости обработки данныхбольших объемов, которые необходимо хранить, а также их многообразия, традиционные SQL-базы данных безопасности не справляются со своей задачей. В данном случае находят применение NoSQL-базы данных.

В работе исследуются следующие виды NoSQL-баз данных:

1. Документоориентированные. Примером таких баз данных являются CouchDB, MongoDB. Моделью данных в таких базах данных является коллекция соединений «ключ-значение», объединенных в документы. Основным преимуществом является возможность работы с разреженными данными. Минусом – низкая производительность запросов к базе данных и отсутствие стандартизированного синтаксиса.
2. Колоночные (HBase, Cassandra). Модель данных – семейства колонок. Такие базы данных предоставляют быструю навигацию по данным, но API в них низкоуровневый.
3. «Ключ-Значение» (Amazon SDB, Redis). Модель данных – коллекция пар «ключ-значение». Обеспечивается быстрый поиск по данным, но хранимые данные в базе данных не имеют схемы.
4. Графовые (Titan DB, Infinite Graph). Модель данных – узлы параметризованного графа. Соответственно, такие базы данных предоставляют все операции по работе с графами, такие как поиск в длину и ширину, поиск кратчайшего пути и т.п. При этом такие базы данных сложнее кластеризовать.

В работе проводится сравнение различных подходов к построению баз данных безопасности и предлагается гибридный подход, позволяющий сочетать использование баз данных SQL и NoSQL. Предлагается комбинированная модель данных безопасности, используемых для мониторинга корпоративной сети, и анализируются возможные реализации этой модели с использованием баз данных SQL и NoSQL.

Работа выполнена при финансовой поддержке РФФИ (проекты 15-07-07451, 16-29-09482 офи_м) и при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007 в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Big Data Analytics for Security Intelligence. Cloud Security Alliance. September 2013. P.1-12.
2. Котенко И.В., Саенко И.Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. № 3 (22). СПб.: Наука, 2012. С.84-100.
3. Котенко И.В., Саенко И.Б. SIEM-системы для управления информацией и событиями безопасности // Защита информации. Инсайд. 2012. № 5 (47). С. 54-65.
4. Котенко И.В., Саенко И.Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. № 1 (24). С. 21-40.
5. Василишин Н.С., Ушаков И.А., Котенко И.В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // В сборнике: Информационные технологии в управлении (ИТУ-2016) Материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В. Г. Пешехонов. 2016. С. 670-675.
6. Apache Hadoop 3.0.0-alpha4 [Электронный ресурс] / URL:http://hadoop.apache.org/docs/current/ (дата обращения 20.09.2017).
7. Котенко И.В., Ушаков И.А. Технологии больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд. 2017. № 3 (75). С. 23-33.

УДК 004.042

ВЛИЯНИЕ ДИНАМИКИ ИЗМЕНЕНИЯ ДАННЫХ НА ПРОЦЕСС КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ

Федорченко Андрей Владимирович[1,2], Котенко Игорь Витальевич[1,2]
[1] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
[2] Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: fedorchenko@comsec.spb.ru, ivkote@comsec.spb.ru

Аннотация. В работе рассматриваются частные задачи процесса корреляции, зависящие от динамики изменения значений свойств событий безопасности. Описываются роль и значимость характеристики динамичности информации в процессе корреляции, а также приводятся примеры влияния на его результат. Оценку динамики изменения значений свойств событий предлагается использовать в рамках структурного и функционального анализов при разработке методики корреляции информации безопасности с возможностью автоматизированной настройки и адаптации к работе в условно неопределенной инфраструктуре.

***Ключевые слова**: корреляция данных, события безопасности, мониторинг безопасности.*

INFLUENCE OF DATA CHANGES DYNAMICS IN THE PROCESS OF SECURITY EVENTS CORRELATION

Fedorchenko Andrey[1,2], Kotenko Igor[1,2]
[1]St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
[2] St. Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University)
Russia, St. Petersburg, Kronverkskiy pr., 49
e-mails: fedorchenko@comsec.spb.ru,ivkote@comsec.spb.ru

Abstract. The paper deals with particular tasks of the process of correlation, which depends on the dynamics of changing the values of the properties of security events. The role and significance of the dynamism of information in the process of correlation are described, and examples of the influence on its result are given. It is proposed to use the assessment of the dynamics of change in event properties values within the framework of structural and functional analysis when developing a methodology for security information correlation with the ability to automatically configure and adapt to operate in a conditionally uncertain infrastructure.

***Keywords:** data correlation, security events, security monitoring.*

За последнее десятилетие угрозы безопасности информационно-телекоммуникационных систем существенно изменились за счет появления новых методов и способов реализации кибератак. Современные атаки на разнообразные критические активы компьютерных инфраструктур зачастую обладают четкой направленностью, достаточной продолжительностью во времени, а также высокой квалификацией действий нарушителей. Текущее поколение средств защиты, как правило, недостаточно эффективно для предупреждения и противодействия подобным атакам, поскольку существующие решения практически не имеют возможности адаптации к настоящим угрозам.

Основополагающим элементом множества классов средств защиты, таких как системы обнаружения (предотвращения) проникновений (Intrusion Detection (Prevention) System, IDS (IPS)), системы предотвращения утечек данных (Data Leak Prevention, DLP), системы управления информацией и событиями безопасности (Security Information and Event Management, SIEM) и других, является компонент корреляции данных. К наиболее важным задачам процесса корреляции относятся: (1) поиск связей между событиями и информацией безопасности; (2) группировка по определенным признакам событий безопасности; (3) обнаружение аномальной и вредоносной активности в анализируемой инфраструктуре [1].

В настоящий момент существует около 20 различных подходов, методов и способов корреляции данных для выполнения задач безопасности [2,3]. Условно все методы корреляции можно разделить на 2 группы: (1) сигнатурные и (2) интеллектуальные. Использование статистического анализа является одним из подходов корреляции данных в обеих группах методов. Однако зачастую существующие методики корреляции разделяют этапы формирования статистических закономерностей и их применение в непосредственных методах корреляции. Данный факт объясняется отсутствием методики адаптации применяемых решений к условно неопределенным инфраструктурам. Например, при использовании результатов статистического анализа данных в сигнатурных методах, требуется участие специалиста для их использования при формировании новых сигнатур (правил, шаблонов, сценариев, моделей и др.). В свою очередь, изменение статистических показателей при их использовании в интеллектуальных методах, требует перестроение и (или) переобучения моделей для выполнения задач корреляции, что требует значительных временных затрат. Также задача адаптации необходима в условиях роста количества и разнообразия обрабатываемой информации (технология больших данных), при которой разделение статистического анализа и применяемых методов может сугубо негативно сказаться как на результатах процесса корреляции, так и на затрачиваемых ресурсах (в том числе времени). Таким образом, глобальная задача заключается в разработке методики корреляции событий и информации безопасности с возможностью автоматизированной настройки и адаптации к условно неопределенной инфраструктуре. Данную задачу предлагается выполнять за счет структурного, функционального, поведенческого и эволюционного анализов [4].

В рамках структурного анализа предлагается обрабатывать исходные данные с целью нахождения прямых и косвенных связей между разными типами событий. Нахождение прямых связей производится путем соответствия идентичных свойств в структуре типов. В свою очередь, определение наличия косвенных однотипных связей является вычислительной задачей, суть которой заключается в пересечении множеств значений свойств друг с другом. Стоит отметить, что данная задача выполняется преимущественно на этапе адаптации компонента корреляции в целевой

инфраструктуре, однако может продолжаться и на этапе эксплуатации. Таким образом, слабая динамика изменения значений свойств событий обратно пропорциональна времени обнаружения косвенных однотипных связей. Также следует учитывать, что все свойства событий могут быть условно разделены на уровни динамичности. Например, свойство типа «Идентификатор процесса» имеет актуальное значение только во время сессии данного процесса, что накладывает ограничения на вычисление актуального множества значений для данного свойства, а уровень данного свойства можно условно назвать «Сессия процесса». Аналогично, свойство типа «Имя пользователя» имеет актуальное значение только во время сессии конкретного пользователя – свойство уровня «Сессия пользователя». Таким образом, характеристика динамики изменения значений свойств и, как следствие, уровней свойств, должна быть обязательно учтена при нахождении косвенных однотипных связей для выполнения процесса корреляции.

Дальнейшее выполнение процесса корреляции подразумевает сравнение значений свойств экземпляров событий для нахождения устойчивых связей между различными типами событий безопасности в рамках функционального анализа исходных данных. Результат данной операции напрямую зависит как от выполнения ранее описанной задачи поиска косвенных связей, так и от динамики изменения значений свойств. В данном случае, слабая и (или) непостоянная динамика изменения значений свойств будет существенно искажать результат определения связи между типами событий безопасности в сторону положительного результата (наличия связи). Для предотвращения возможности описанной погрешности следует вычислять характеристику динамичности изменения значений свойств событий и учитывать ее при определении временного окна (репрезентативной выборки из генеральной совокупности) для выполнения процесса корреляции.

Исходя из вышеизложенного, следует заключить, что динамика изменения значений свойств событий безопасности является важной характеристикой в процессе корреляции, поскольку оказывает на него непосредственное влияние на этапе структурного и функционального анализов. Дальнейшим направлением исследований является разработка методики вычисления и оценки динамики изменения значений свойств, а также определение уровней динамичности свойств событий безопасности.

Работа выполнена при финансовой поддержке РФФИ № 16-37-00338-мол_а, № 15-07-07451-а и при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007 в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1 // Труды СПИИРАН. 2016. Вып. 47. С.5-27.
2. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах.Часть 2 // Труды СПИИРАН. 2016. Вып. 6(49). С.5-27.
3. A. Muller, “Event Correlation Engine,” Master`s Thesis. Swiss Federal Institute of Technology Zurich. 2009. 165 p.
4. A. Fedorchenko, I. Kotenko, D. El Baz, “Correlation of Security Events based on the Analysis of Structures of Event Types”, Proceedings of the 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS’2017), 2017.pp 270-276.

УДК 004.042

ФОРМАТЫ СОБЫТИЙ БЕЗОПАСНОСТИ В ПОДСИСТЕМЕ ЖУРНАЛИРОВАНИЯ ОС WINDOWS

Федорченко Андрей Владимирович[1,2], Чечулин Андрей Алексеевич[1,2],
Дойникова Елена Владимировна[1,2]
[1] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
[2] Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: fedorchenko@comsec.spb.ru, chechulin@comsec.spb.ru, doynikova@comsec.spb.ru

Аннотация. Представленная работа посвящена исследованию форматов описания событий безопасности в операционных системах семейства Windows. Рассматриваются способы и особенности получения информации из подсистемы журналирования данных операционных систем с целью их дальнейшего использования в классе средств управления событиями и информацией безопасности. Рассматриваются форматы описания событий безопасности, их преимущества и недостатки при различных вариантах обработки в качестве исходных данных. Также приводятся результаты анализа содержимого событий безопасности и его влияния на процесс оценки защищенности компьютерных инфраструктур.

Ключевые слова*: форматы данных; события безопасности; подсистема журналирования; ОС Windows.*

SECURITY EVENT FORMATS IN LOGGING SYSTEM OF OS WINDOWS

Fedorchenko Andrey[1,2],Chechulin Andrey[1,2],Doynikova Elena[1,2]
[1]St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
[2] St. Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), Russia, St. Petersburg, Kronverkskiy pr., 49
e-mails: fedorchenko@comsec.spb.ru, chechulin@comsec.spb.ru, doynikova@comsec.spb.ru

Abstract. The presented work is devoted to the study of formats for describing security events in operation systems of the Windows family. The ways and peculiarities of obtaining information from the data log subsystem of operating systems ith the purpose of their further use in the class of monitoring and security management tools are considered. The formats for describing security events, their advantages and disadvantages in various processing options as input data are considered. Also, the results of the analysis of the contents of security events and its impact on the process of assessing the security of computer infrastructures are presented.

Keywords: *.data formats, security events, log subsystem, OS Windows.*

В настоящее время информационные технологии применяются практически во всех сферах человеческой жизнедеятельности: государственном управлении, промышленности, транспортном и энергетическом комплексах, коммунальных сервисах, силовых ведомствах, финансовом секторе, бизнесе и личном использовании. В связи с данным фактом, на фоне роста уровня угроз информационной безопасности, увеличивается степень необходимой защиты компьютерных инфраструктур, особенно в критически важных объектах. Последние исследования [1] показывают, что в текущий момент наиболее востребованными являются мобильные операционные системы, однако их применение ограничивается преимущественно личным пользованием, не относящимся к рабочим процессам. Вместе с тем, самыми популярными настольными операционными системами остаются решения семейства Windows, также имеющие возможность применения во встраиваемых системах.

Одним из способов мониторинга уровня защищенности компьютерных инфраструктур является анализ событий безопасности, регистрируемых, в том числе, используемыми операционными системами. Один з классов средств защиты информации, в которых используется данных способ, представлен системами управления информацией и событиями безопасности (SecurityInformationandEventManagement, SIEM) [2]. Суть работы таких решений основан на сборе различной информации и событий и последующей обработке с целью выявления предупреждений и инцидентов безопасности.

Основным элементом сбора, предварительной обработки и анализа событий безопасности является компонент корреляции. Наиболее важными этапа процесса корреляции являются: (1) нормализация; (2) анонимизация; (3) фильтрация; (4) агрегация; (5) корреляция и (6) ранжирование [3]. Первоначальным и достаточно важным этапом обработки событий является нормализация, поскольку исходные данные для их дальнейшей корреляции собираются от множества разнородных источников. Уже на данном этапе целесообразно применять шаблонные методы предварительной обработки данных [4], позволяющие минимизировать различия между форматами событий безопасности, что повышает эффективность выполнения всех последующих этапов.

Операционные системы семейства Windows линейки NT имеют достаточно развитую и настраиваемую подсистему журналирования. В данной подсистеме присутствует 5 основных журналов событий с различными правами доступа: (1) приложений; (2) системы; (3) безопасности; (4) установки; (5) переадресованных событий. Для доступа к событиям и конфигурации 1, 2 и 3 журналов требуются права администратора системы. Сбор событий безопасности возможен двумя способами: (1) ручной, через штатное средство просмотра и сохранения событий в файл; (2) программный, с помощью вызова определенных API-функций. Стоит отметить, что первый вариант не подходит для автоматизированного сбора событий, поскольку требует выполнения всех операций администратором безопасности, а также дополнительной синхронизации собранных данных. В свою очередь, второй способ является достаточно надежным для автоматизированного сбора, а также дальнейшей обработки исходных данных.

Описанные варианты сбора событий безопасности имеют возможность представления данных в 5-и форматах. Первый способ, по заявленным характеристикам разработчиков, позволяет сохранять события в 4х форматах: (1) «*.evtx» - формат базы данных журнала событий ОС Windows; (2) «*.xml» - расширяемый язык разметки (eXtensible Markup Language); (3) «*.txt» - текстовый файл; (4) «*.csv» - значения, разделённые запятыми (Comma-SeparatedValues). Первый формат является основным для хранения журналов событий в операционных системах семейства Windows и не имеет официально открытой спецификации. Несмотря на наличие готовых программ обработчиков, данный формат не является пригодным для сбора событий безопасности и последующей обработки ввиду возможности его непредсказуемого изменения разработчиками, например, в ходе очередного обновления. Второй формат событий представляет данные в полуструктурированном виде и позволяет

автоматизированную обработку, однако имеет существенный недостаток: специфичные свойства событий не имеют групповой иерархии, что снижает эффективность его применения и увеличивает сложность нормализации исходной информации. Текстовый формат (3) является наиболее информативным и удобным для человеческого восприятия, однако сложен в обработке, поскольку зависит от используемого языка в системе. Четвертый формат по факту представляет данные согласно спецификации (с помощью разделителя) только основных свойств, тогда как все специфичные свойства не отличаются от текстового варианта и не удовлетворяют требованиям формата, что также практически не позволяет использовать его в автоматизированном сборе и последующей обработке. С помощью API вызовов, обрабатывающих журналы событий, представляется возможным автоматизированный сбор событий безопасности в 5 формате. Основные свойства событий в данном формате имеют структурированный вид, что позволяет их дальнейшую обработку без дополнительных преобразований. В свою очередь, дополнительные свойства событий в данном формате представлены в текстовом виде с групповой иерархией свойств, что вносит дополнительную точность при их дальнейшей обработке. Также следует отметить, что представление данных в текстовом виде производится с разыменованием значений ряда полей. Например, в формате «*.xml» поле «LayerName» имеет значение «%%14608», что является неразыменованной константой, представленной в текстовом виде разыменованным значением «Resource Assignment». Данное отличие позволяет заключить, что сбор событий безопасности в формате «*.xml» является менее удобным для человеческого восприятия, тогда как при автоматизированной обработке 5го формата, текстовое описание ведет к незначительно большему расходу памяти.

Проведенные исследования показали, что наиболее приемлемым для выполнения задач корреляции является использование программного способа сбора событий безопасности, поскольку получаемые с его помощью исходные данные позволяют минимизировать их обработку с сохранением точности представляемой информации. Также стоит отметить, что для работы в режиме реального времени и автоматизации сбора событий безопасности, единственным приемлемым вариантом выступает программный способ через вызовы системных API-функций.

Работа выполнена при поддержке Гранта президента Российской Федерации (МК-314.2017.9).

СПИСОК ЛИТЕРАТУРЫ

1. Рейтинг операционных систем: июнь 2017. Веб-сайт ITRew.ru [Электронный ресурс]. Режим доступа: http://www.itrew.ru/windows/reyting-operacionnykh-sistem-iyun-2017.html (по состоянию на 25.09.2017).
2. Котенко И.В., Саенко И.Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. № 3 (22). СПб.: Наука, 2012. С.84-100.
3. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1 // Труды СПИИРАН. 2016. Вып. 47. С.5-27.
4. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах.Часть 2 // Труды СПИИРАН. 2016. Вып. 6(49). С.5-27.

УДК 004.056.53

УГРОЗЫ БЕЗОПАСНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ И ЗАЩИТА ОТ ИНФОРМАЦИИ

Проноза Антон Александрович, Чечулин Андрей Алексеевич,
Комашинский Николай Александрович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mails: pronoza@gmail.com, chechulin@comsec.spb.ru, nckkm@yandex.ru

Аннотация. В работе рассматриваются актуальные угрозы, возникающие в следствии широкого распространения социальных сетей. Предложена классификация угроз в зависимости от их источника, среды распространения, вида передаваемой информации и целевого объекта. Приведены примеры, указывающие на важность рассмотрения вопросов защиты от информации наряду с информационной безопасностью.

Ключевые слова: *социальные сети; информационная безопасность; защита от информации.*

SECURITY THREATS IN SOCIAL NETWORKS AND PROTECTION FROM INFORMATION

Pronoza Anton, Chechulin Andrey, Komashinsky Nikolay
St. Petersburg Institute for Informatics and Automation of Russian Academy ofSciences
Russia, St. Petersburg, 14 Liniya, 39
e-mails: pronoza@gmail.com, chechulin@comsec.spb.ru, nckkm@yandex.ru

Abstract. The paper describes actual threats coming from social networks. The classification of threats depending on source, environment, type of information and target is proposed. Examples of importance considering both protection from information and information security are given.

Keywords: *social networks; information security; protection from information.*

Традиционно под информационной безопасностью понимают такое состояние информации, при котором обеспечивается ее целостность, доступность и конфиденциальность. Однако сегодня существуют технологии, изменившие привычные правила информационного обмена.

Появление концепции «Web 2.0», а вслед за ней и различных социальных площадок, где пользователи могут не только свободно обмениваться информацией, но и выкладывать ее в общий доступ, приводит к появлению так называемой «публичной» информации, основной целью создания которой является ее дальнейшее распространение. К таким площадкам относятся: видеохостинг «Youtube», сервис микроблогов «Twitter», сетевое сообщество «LiveJournal», социальные сети «Facebook», «ВКонтакте» и др.

Постепенно социальные сети из простой площадки по обмену информацией и объединению сообществ по интересам становятся полноценной платформой по противостоянию между различными субъектами, начиная от рекламщиков и малого бизнеса, и заканчивая криминальными структурами и крупными геополитическими игроками.

Классификация угроз. В связи с этим представляется целесообразным классифицировать угрозы, исходящие от социальных площадок и показать, что часть из них частично отличается от привычного понимания информационной безопасности. Так, например, большая часть публикуемых пользователями сведений доступна для всех, а их колоссальные объемы и незначительность источника распространения зачастую делают бессмысленными попытки провести атаку на саму информацию или скомпрометировать ее источник. В то же время нерешенным остается вопрос о состоянии информационной защищенности человека, являющегося конечным потребителем информации.

Публикуемые другими пользователями сети текстовые сообщения с привязанным мультимедиа контентом способны оказывать негативное влияние на сознание и психику читателя, вводить его в заблуждение, навязывать определенную точку зрения, призывать к противоправной деятельности, угрожать его жизни и здоровью или иным образом ограничивать его права и свободы.

Угрозы информационной безопасности, исходящие от социальных сетей, целесообразно представлять в виде четырех компонент: источник угрозы, среда распространения потенциально опасной информации, сама информация и цель, которой она адресована.

Источником угрозы может быть пользователь, группа людей или государство. При этом необходимо учитывать, что источником угрозы может выступать как непосредственно человек, например, организатор так называемой «группы смерти», так и скомпрометированный аккаунт пользователя, осуществляющий рассылку спама или занимающийся вымогательством среди «друзей» аккаунта. Группа людей способна проводить более массовые и скоординированные атаки на конечных потребителей информации, что характерно для радикально настроенных группировок, стремящихся к распространению своих идей и приобретению новых членов.

Угрозы, исходящие от одного государства по отношению к другому, в настоящее время недостаточно изучены, однако представляется уместным в данном случае упомянуть, что помимо больших денежных ресурсов и популярных официальных аккаунтов должностных лиц могут использоваться и иные способы массовой манипуляции мнениями пользователями социальной сети.

Под средой распространения информации следует понимать возможности, которыми обладает злоумышленник для реализации своих угроз. К таким возможностям следует отнести популярные сервисы социальных сетей, позволяющие публиковать сообщения для неограниченного круга лиц, создавать сообщества, приглашать на встречи и т.п.

Отдельно следует упомянуть о возможности использования ботов, способных на массовый информационный вброс с одновременным использованием множества сервисов.

Передаваемую через социальную среду потенциально опасную информацию можно разделить на четыре категории: заведомо ложная информация (например, «фейковые» новости, информационные вбросы), нежелательная информация (например, имеющая ограничения по возрасту), информация, запрещенная к распространению (например, возбуждение расовой ненависти, публичное оправдание терроризма [7]) и информация технического характера (например, вредоносные ссылки, распространение спама).

Целью при реализации описанных выше угроз путем передачи потенциально опасной информации могут выступать как человек, общество и государство, так и компьютер пользователя.

Базовые инструменты социальной сети делают относительно простой для злоумышленника задачу влияния на большие массы людей. Например, такие инструменты могут применяться для организации одновременных массовых мероприятий в различных городах страны. Как результат подобного воздействия, человек оказывается под информационно-психологическим влиянием.

Защита от информации. Основные положения по борьбе с потенциально опасной информацией приводятся в Доктрине информационной безопасности Российской Федерации, в которой в качестве основных информационных угроз наряду с компьютерными атаками рассматривается в том числе и информационно-психологическое воздействие, осуществляемое специальными службами отдельных государств [8]. Например, распространение запрещенной информации, такой как экстремистская

литература или детская порнография, блокируется уполномоченными на то федеральными органами исполнительной власти и преследуется в соответствии с Уголовным Кодексом [6].

Для борьбы с заведомо ложной информацией и «фэйковыми» новостями государственные органы создают интернет ресурсы с соответствующими опровержениями [11]. Для борьбы с вредоносной информацией технического характера применяется специализированное программное обеспечение и интеллектуальные алгоритмы анализа данных, такие как [9, 10].

В настоящее время влияние социальных площадок возрастает. Пользователи социальных сетей ежедневно потребляют привычный для них контент без должного критического отношения. Все это становится особенно критичным для подростков, среду развития которых определяют сообщества, на которые они подписаны.

Данные факты обуславливают необходимость обеспечивать не только безопасность самой информации, но и защиту от информации, для гарантии того, что интересы личности, общества или государства не были нарушены. При этом, необходимо отметить, что защита от информации носит междисциплинарный характер.

В тех случаях, когда информация может нанести вред, должны срабатывать соответствующие механизмы защиты. В силу стремительного развития средств связи и возможностей обмена информацией можно утверждать, что сегодня защита от информации является необходимой компонентой безопасности общества и государства.

Работа выполнена при финансовой поддержке РФФИ (проекты 15-07-07451, 16-29-09482 офи_м) и при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007 в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.07.2017) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954., ст. 280.
7. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» (ред. от 23.11.2015) // Собрание законодательства Российской Федерации от 2002. № 30. Ст. 3031.
8. Указ Президента Российской Федерации от 05.12.2016 г. №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст.7074.
9. Комашинский Д.В., Котенко И.В., Чечулин А.А., Шоров А.В. Автоматизированная система категорирования веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Системы высокой доступности, № 3 (9), 2013. С.119-127.
10. Igor Kotenko, Andrey Chechulin, Andrey Shorov, Dmitry Komashinsky. Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking. P. Perner (Ed.): 14th Industrial Conference on Data Mining (ICDM 2014), Lecture Notes in Artificial Intelligence (LNAI 8557), DOI 10.1007/978-3-319-08976-8. P.39–54.
11. Примеры публикаций, тиражирующих недостоверную информацию о России [Электронный ресурс] // Министерство иностранных дел Российской Федерации. Официальный сайт. URL: http://www.mid.ru/nedostovernie-publikacii. Дата обращения: 23.09.2017.

УДК 004.056.53

АВТОМАТИЧЕСКОЕ ВЫЯВЛЕНИЕ РАЗЛИЧИЙ В ИНТЕРЕСАХ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНОЙ СЕТИ В ЗАВИСИМОСТИ ОТ УКАЗАННЫХ ИМИ ПСИХИЧЕСКИХ ФУНКЦИЙ

Проноза Антон Александрович[1], Проноза Екатерина Валерьевна[2], Чечулин Андрей Алексеевич[1], Котенко Игорь Витальевич[1]

[1] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39

[2] Санкт-Петербургский государственный университет
Россия, Санкт-Петербург, Университетская наб., 7/9

e-mails: pronoza@gmail.com, katpronoza@gmail.com, chechulin@comsec.spb.ru, ivkote@comsec.spb.ru

Аннотация. В работе приводятся основные этапы и результаты работы разработанного алгоритма извлечения зависимости круга интересов пользователей социальной сети от сведений, размещаемых ими на своих страницах. В качестве таких сведений в настоящем исследовании выступают психические функции Юнга, на которые пользователь неявно ссылается путем вступления в соционические сообщества.

Ключевые слова: *социальные сети; типология Юнга.*

AUTOMATIC DETECTION OF DIFFERENCE BETWEEN THE INTERESTS OF SOCIAL NETWORK USERS OF DEPENDING ON THEIR COGNITIVE FUNCTIONS

Pronoza Anton[1], Pronoza Ekaterina[2], Chechulin Andrey[1], Kotenko Igor[2]

[1] St. Petersburg Institute for Informatics and Automation of Russian Academy ofSciences
Russia, St. Petersburg, 14 Liniya, 39

[2]St. Petersburg State University, Russia, St. Petersburg, 7/9 Universtitetskaya nab.

e-mails: pronoza@gmail.com, katpronoza@gmail.com, chechulin@comsec.spb.ru, ivkote@comsec.spb.ru

Abstract. The paper proposes an algorithm of automatic detection of differences between the interests of social network users depending on the information they publish on their pages. Such information

is represented by the cognitive functions introduced by Jung. Users implicitly refer to such functions by joining specific social network communities devoted to the Socionics theory.

Keywords: *social networks; Jungian cognitive functions.*

Социальные сети в настоящее время являются одним из наиболее распространенных способов рассказать о себе и своих увлечениях, найти друзей-единомышленников, получать персонализированный контент. Профиль в социальной сети становится отражением личности и ее интересов, и зачастую говорит о человеке больше, чем он может рассказать о себе при реальной встрече.

Принадлежность пользователя к определенным сообществам указывает не только на его интересы и ценности, но и в определенной мере показывает, как он позиционирует себя в обществе и кем он ощущает себя в современном мире. В частности, к попыткам самоопределения можно отнести декларацию пользователем своей принадлежности к узким тематическим сообществам, разбивающим все множество людей на ограниченное число не пересекающихся кластеров. Этот факт, в свою очередь, делает возможным выявление круга особо выраженных интересов, присущих только лицам данного тематического сообщества. В дальнейшем, это позволит прогнозировать принадлежность личности к узкому тематическому сообществу по выраженности ее интересов на персональной странице, аналогично [1].

Целью данной работы является анализ интересов пользователей социальных сетей по тому, как они сами определяют свои психические функции. Исследование проводится на примере пользователей социальной сети «ВКонтакте», а интересы пользователей определяются на основе анализа сообществ, в которых он состоит. Для формирования групп пользователей была выбрана классификация психологических типов личности, разработанная швейцарским психиатром К. Г. Юнгом и описанная им в работе «Психологические типы».

Типология К. Г. Юнга получила широкое распространение среди людей, в том числе не связанных с научным сообществом. Одним из наиболее известных ответвлений является соционика. Основные положения соционики разделяют людей на 16 соционических типов информационного метаболизма, которые, в свою очередь, опираются на психологические установки и функции К. Г. Юнга. Для определения своего типа существует множество несложных тестов, которые позволяют пользователю отнести себя к той или иной соционической группе. При этом нередко пользователи социальной сети, определив свой тип, вступают в соответствующие тематические сообщества и делятся результатами тестов со своими друзьями.

В данном исследовании предполагается, что большинство людей, состоящих в таких сообществах, верно определили свою психическую функцию. Например, если человек состоит в группе «ИЛЭ» (интуитивно-логический экстраверт), значит в нем преобладают функции мышления и интуиции, в противоположность функциям чувств и ощущений.

В данной работе проводился сравнительный анализ интересов пользователей, у которых преобладает функция интуиции, с теми пользователями, у которых преобладает функция ощущения. Предполагается, что эти интересы выражены теми сообществами, на которые пользователи подписаны. Кроме того, было сделано предположение, что тематика любого сообщества социальной сети «ВКонтакте» определяется его заголовком и описанием.

Для проведения исследования были выбраны 16 сообществ, соответствующих 16 соционическим типам информационного метаболизма. Из указанных сообществ одна половина соответствует типам с преобладанием функции ощущений, а другая – функции интуиции. Всего было исследовано более 40 000 носителей каждой функции.

По каждой группе носителей собираются все сообщества, в которых они состоят. При этом был учтен тот факт, что разные пользователи могут состоять в одинаковых сообществах. Продублированные сведения позволяют сохранить распределение ключевых слов, соответствующих пользовательским интересам. Названия сообществ и их описания образуют текстовую коллекцию, из которой исключаются все части речи, за исключением имен существительных. Таким образом, в результате были сформированы два корпуса, состоящих из имен существительных, тем или иным образом указывающих на интересы пользователей из исследуемых групп.

В процессе работы для каждого корпуса был сформирован частотный словарь, на основе которого были выбраны наиболее часто встречающиеся слова. Далее, для объединения сходных по смыслу и значению слов в единый кластер был использован разработанный авторами алгоритм семантической кластеризации [5]. Для определения степени сходства слов учитывалась степень их близости в соответствии с технологией «word2vec» [4] и тезаурусом синонимов [3], а также однокоренными словами [1]. Необходимые численные параметры для алгоритма кластеризации подбирались эмпирическим путем.

Полученные кластеры соответствуют основным тематикам, встречающимся в исследованных корпусах, при этом тематика определяется вручную произвольным словом, входящим в кластер и наиболее полно его описывающим. В частотных словарях слова, входящие в полученные кластеры, заменяются на соответствующие тематики. Частота тематики вычисляется как сумма частот слов,

входящих в соответствующий кластер. В конечном итоге формируются отсортированные по частоте встречаемости тематики для каждой группы пользователей.

Для того чтобы определить различия в интересах групп пользователей, вычисляется разность между частотами соответствующих тематик из разных корпусов. Соответственно, чем меньше по модулю вычисляемая разность, тем больше похожи интересы двух групп, и наоборот.

В результате исследования было установлено, что группа пользователей с преобладающей функцией интуиции, в отличие от пользователей с противоположной функцией, интересуется следующими категориями: «музыка», «кинематограф», «искусство», «литература», «астрология». Интересами группы пользователей с ярко выраженной функцией ощущений, в противоположность первой группе, стали категории «аниме», «театры/музеи/телешоу» (указанные существительные оказались в одном кластере) и «здоровье». Полученные результаты не противоречат представлениям о людях с указанными целевыми функциями.

В настоящем исследовании выявлялись зависимости между выраженностью психологических функций личности и тематикой сообществ, в которых она состоит. Результаты, полученные в ходе настоящего исследования, в дальнейшем будут использованы для проверки гипотезы, согласно которой по выявленным интересам пользователя можно сделать вывод о психологических свойствах его личности.

Работа выполнена при финансовой поддержке РФФИ (проекты 15-07-07451, 16-29-09482 офи_м) и при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007 в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Комашинский Д.В., Котенко И.В., Чечулин А.А., Шоров А.В. Автоматизированная система категорирования веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Системы высокой доступности, № 3 (9), 2013. С.119-127.
2. Тихонов А. Н. Словообразовательный словарь русского языка в двух томах: ок. 145000 слов. М.: Русский язык, 1985.
3. Braslavski P., Ustalov D. and Mukhin M. A spinning wheel for YARN: user interface for a crowdsourced thesaurus, in proc. of the Demonstrations at the 14th Conference of the European Chapter of the Association for Computational Linguistics, Gothenburg, Sweden, 2014, pp. 101–104.
4. Mikolov T., Chen K., Corrado G. S. and J. Dean J. Efficient estimation of word representations in vector space, web: http://arxiv.org/abs/1301.3781/, 2013.
5. Pronoza E., Yagunova E., Pronoza A. Construction of a Russian Paraphrase Corpus: Unsupervised Paraphrase Extraction. Proceedings of the 9th Russian Summer School in Information Retrieval, August 24–28, 2015, St. Petersburg, Russia, (RuSSIR 2015, Young Scientist Conference), Springer CCIS, vol. 573, pp. 146-157, 2016.

СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056.53

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ VGATE R2

Бородин Михаил Константинович, Бородина Полина Юрьевна
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: mikborod@gmail.com, p.y.zakharova@gmail.com

Аннотация. В данной статье описано проведение тестирования на проникновение современного средства защиты виртуализации vGateR2 4.0, установленного на стенде с виртуальной инфраструктурой на основе VMwarevSphere. Цель тестирования состояла в обнаружении потенциальных уязвимостей в защите виртуальной инфраструктуры без нанесения вреда непосредственно виртуальным машинам. Работа проводилась с применением методов тестирования чёрного и серого ящиков. В ходе исследования были использованы утилиты и приложения из KaliLinux — популярного дистрибутива для проведения подобного тестирования. Особое внимание было уделено утилитам для сканирования и создания нагрузки на сетевую инфраструктуру, в частности, описано использование известной утилиты Nmap, сначала для сканирования сети и получения информации о возможных уязвимостях, а затем для проведения атаки типа «отказ в обслуживании» в связке с утилитой hping3.

Ключевые слова: *тестирование на проникновение; виртуализация; СЗИ vGateR2; KaliLinux; VMware.*

PENETRATION TESTING OF DATA PROTECTION SUITE VGATE R2

Borodin Mihail, Borodina Polina
ITMO University
Russia, St. Petersburg, Kronverkskiy pr., 49
e-mails: mikborod@gmail.com, p.y.zakharova@gmail.com

Abstract. This research paper describes the process of penetration testing of a modern virtualization protection suite vGate R2 4.0 installed on a pre-deployed stand with a virtual infrastructure based on VMware vSphere. The purpose of this testing is to detect potential vulnerabilities in the virtual infrastructure protection without directly damaging virtual machines. We had conducted penetration testing by the methods of black and gray boxes. We will use various utilities and applications from Kali Linux distribution for scanning the network infrastructure and load testing. Special attention was paid to utilities for scanning and creating loads on the network infrastructure, in particular, the use of Nmap utility is described not only as a means of information gathering, but also as an additional tool for implementing a denial-of-service attack in conjunction with the hping3 utility.

Keywords: *penetration testing; virtualization; vGate R2; Kali Linux; VMware.*

Введение. Тестирование на проникновение является важным направлением в проведении аудита информационной безопасности. Под термином «тестирование на проникновение» подразумевается имитация возможных действий злоумышленника, преследующего цель получения несанкционированного доступа к информационной системе. Такое тестирование позволяет получить объективную оценку защищённости системы от возможного злоумышленника, посмотреть на систему с его точки зрения и понять, какие места системы нуждаются в дополнительной защите [1].

Выбор методики тестирования

Для проведения тестирования была разработана методика на основе двух существующих методик: NIST Special Publication 800-115 [2], разработанной подразделением NIST CSRC и методики Богораза А.Г. и Песковой О.Ю., созданной для тестирования межсетевых экранов [3].

Используемая методика включает в себя следующие этапы:

1. Планирование. Определяются тестируемые цели и условия проведения тестирования.
2. Подготовка. Производится сборка тестового стенда и настройка тестовой среды.
3. Исследование. Начало тестирования: сбор информации о системе, сканирование сетевой инфраструктуры и использование сканеров уязвимостей.

4. Атака. Использование ранее собранных данных для проведения атаки.

5. Отчёт. Создание отчёта с описанием уязвимостей, оценкой рисков и возможными рекомендациями по смягчению обнаруженных недостатков.

Описание тестового стенда

Перед проведением тестирования была изучена документация к продукту [4] и определена необходимая конфигурация тестового стенда. Было решено проводить тестирование с использованием методом чёрного и серого ящиков.

Во время тестирования на проникновение по методу чёрного ящика [5] в качестве атакующей системы был выбран дистрибутив Kali Linux на ноутбуке с внешней всенаправленной Wi-Fi антенной повышенного усиления. В качестве целей для атаки использовались: сервер под управлением операционной системы Windows Server 2012R2 с установленным Сервером авторизации vGate [4], аппаратный гипервизор vSphere ESXi 5.5 и точка доступа Asus RT-N12, объединенные в локальную сеть, схема которой представлена на рисунке 1.

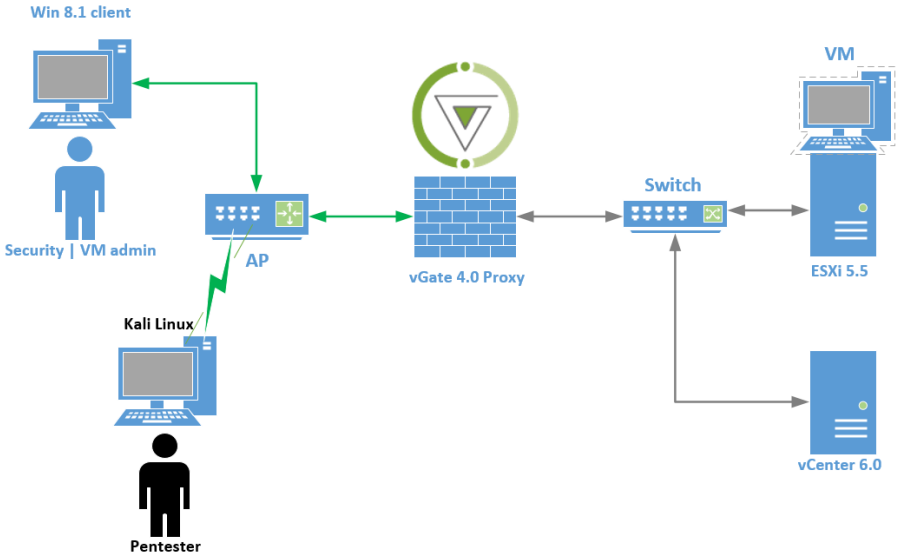


Рис. 1. Общая схема собранного тестового стенда

На рисунке 1 – схема сети разделена на две части: подсеть администрирования (слева) и защищаемая подсеть виртуализации (справа).

Моделирование действий злоумышленника при тестировании на проникновение по методу серого ящика производилось с операционной системы Windows 8.1 с установленным Агентом аутентификации vGate[4], в распоряжении злоумышленника находилась учётная запись администратора виртуализации с ограниченными правами на управление инфраструктурой. Основной целью, в данном случае, являлось повышение привилегий текущего пользователя или захват учётной записи администратора безопасности для доступа к консоли управления СЗИ vGateR2, интерфейс которой представлен на рисунке 2.

Тестирование по методу чёрного ящика

Вначале производится проникновение в локальную сеть организации дистанционно используя известные уязвимости стандарта защиты беспроводных сетей Wi-Fi стандарта WPA2. По сей день на многих предприятиях используется именно этот стандарт с настройками безопасности, потерявшими свою актуальность [6]. Даже высокая сложность пароля не может больше гарантировать безопасность точки доступа, так как были открыты способы быстрого перебора с использованием мощностей графических ускорителей и радужных таблиц, а необновленное сетевое оборудование может быть скомпрометировано по новейшей методике Key Reinstallation Attacks за считанные минуты[7]. Скрытие имени сети (SSID) и включение фильтрации по MAC адресам также слабо сказываются на защищенности подключения.

После подключения к сети был произведён предварительный сбор информации путём анализа сетевого трафика программой Wireshark в «неразборчивом» режиме, в результате которого были получены IP и MAC адреса серверов, клиента и точки доступа, а также их NetBIOS имена и название домена используемого внутри подсети виртуализации.

Далее была применена утилита Nmap, предназначенная для настраиваемого сканирования IP-сетей и определения состояния объектов сканируемой сети. В штатном режиме работы СЗИ vGateR2 полноценному сканированию подвержен только клиент, видны типичные для ОС Windows 7/8 открытые порты, операционная система корректно определяется утилитой с использованием отпечатков стека TCP/IP. Сканирование сервера авторизации vGateR2, работающего в режиме

шлюза, показывает открытыми только нетипичные для Windows порты 3800/TCP и 3801/TCP, отпечаток стека утилите неизвестен. Вывод данной утилиты показан на рисунке 3.

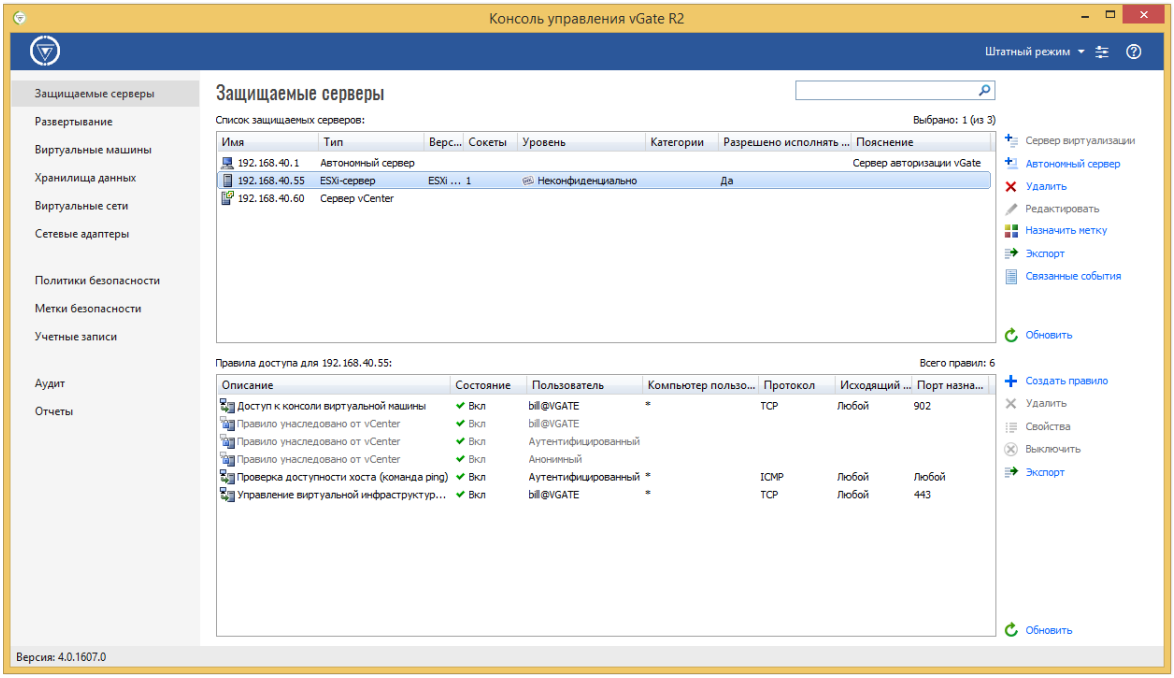


Рис. 2. Консоль управления vGate R2

Остальные сервера недоступны для сканирования утилитой Nmap, не отвечают на ICMP запросы и невидимы для сканеров уязвимостей из дистрибутива KaliLinux.

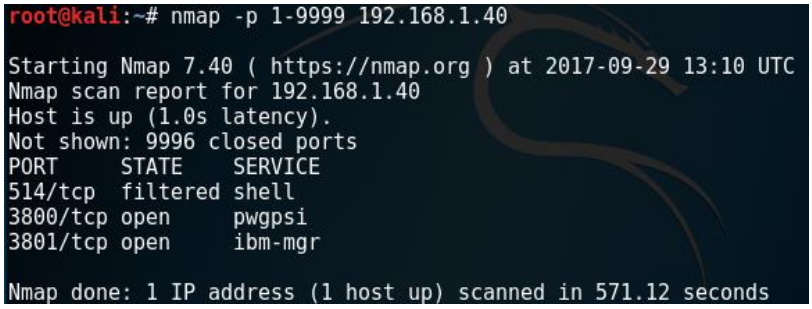


Рис. 3. Сканирование сервера авторизации vGate R2 с помощью утилиты Nmap

После сбора доступной информации была предпринята попытка атаки по словарю на форму входа аппаратного гипервизора ESXi 5.5 при помощи утилиты Hydra, предназначенной для проведения взлома сетевого входа в систему с применением различных протоколов. В аварийном режиме работы СЗИ vGateR2[4] данная атака реализуема и показывает эффективную скорость перебора около 16 паролей в минуту (рисунок 4), однако, в штатном режиме работы[4] атака блокируется и утилита завершается с ошибкой подключения (рисунок 5).

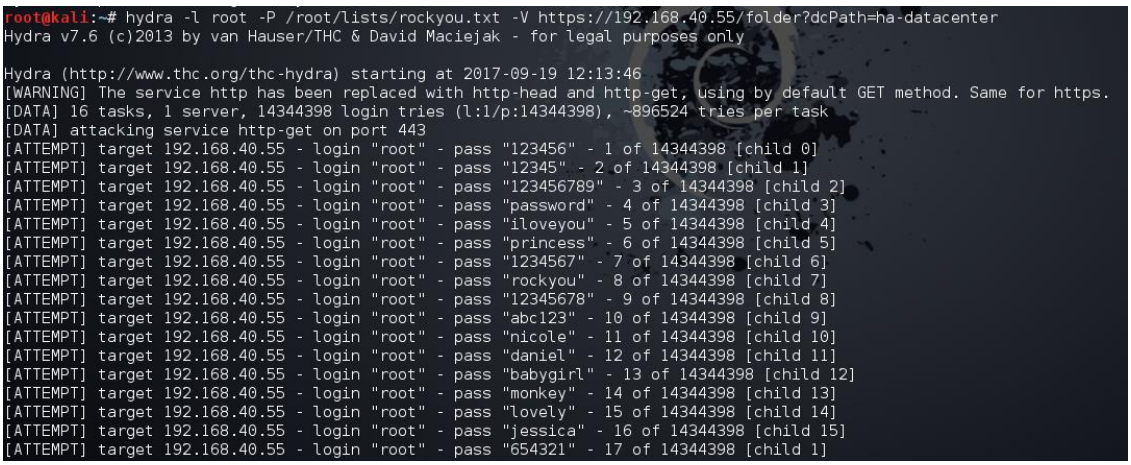


Рис. 4. Реализация атаки перебором по словарю с помощью утилиты Hydra

```
[VERBOSE] Disabled child 1 because of too many errors
[ERROR] Too many connect errors to target, disabling http-get://192.168.40.55:443
0 of 1 target completed, 0 valid passwords found
[ERROR] 1 target did not resolve or could not be connected
```

Рис. 5. Ошибка подключения утилиты Hydra к серверу ESXi

Далее была проведена атака типа «отказ в обслуживании» на сервер авторизации vGateR2 с помощью утилиты hping3, предназначенной для создания высокой нагрузки на сетевую инфраструктуру. На рисунке 6 показано применение утилиты hping3 для создания высокой SYN-flood нагрузки. Также, для создания дополнительной нагрузки с высокой степенью фрагментации и пакетами большого размера была использована утилита Nmap, что отражено на рисунке 7.

```
root@kali:~# hping3 -S 192.168.1.40 -i u1 -p 443
HPING 192.168.1.40 (wlan2 192.168.1.40): S set, 40 headers + 0 data bytes
^C
--- 192.168.1.40 hping statistic ---
29187 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Рис. 6. Создание сетевой нагрузки утилитой hping3

```
root@kali:~# nmap -v --mtu 8 --data-length 30000 --badsum 192.168.1.40
WARNING: Payloads bigger than 1400 bytes may not be sent successfully.

Starting Nmap 6.40 ( http://nmap.org ) at 2017-09-20 19:18 MSK
Initiating ARP Ping Scan at 19:18
Scanning 192.168.1.40 [1 port]
Completed ARP Ping Scan at 19:18, 0.59s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Nmap scan report for 192.168.1.40 [host down]
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.74 seconds
           Raw packets sent: 2 (56B) | Rcvd: 0 (0B)
```

Рис. 7. Создание сетевой нагрузки утилитой Nmap

Результатом проведения атаки только при помощи hping3 были: высокая нагрузка на сетевой адаптер и полная загрузка ядер ЦПУ сервера авторизации, что провоцировало затруднения при подключении клиентов и общее падение производительности системы. Дополнительно было выявлено, что при использовании на сервере авторизации сетевого адаптера Wi-Fi компании Qualcomm Atheros для подключения к точке доступа в подсети администрирования, и совместной нагрузке утилит hping3 и Nmap, возникает возможность спровоцировать критическую ошибку Windows, известную как «синий экран смерти», с генерацией дампа памяти и последующей перезагрузкой. Данная уязвимость не влечёт нарушения целостности системы безопасности инфраструктуры виртуализации, но позволяет добиться полного краткосрочного отказа в обслуживании для всех администраторов виртуализации и безопасности. Её недостатком является невозможность эксплуатации совместно с другими сетевыми картами, в частности с проводными Ethernet адаптерами Intel и Atheros.

Тестирование по методу серого ящика

При тестировании на проникновение в данном случае моделируемый злоумышленник имел доступ к клиентской рабочей станции, информацией об общем устройстве системы и сети, а также обладал учётными данными администратора виртуализации с ограниченными правами на управление инфраструктурой.

Была предприняты попытки перебора пароля для учётной записи администратора безопасности vGateR2, через интерфейс агента аутентификации и встроенную утилиту clacl.exe, которые привели к блокированию данной учётной записи после трёх неудачных попыток, так как для соединения использовалась имплементация протокола безопасности Kerberos 5.

Также была осуществлена неудавшаяся попытка запуска консоли управления через соответствующий исполняемый файл, расположенный в каталоге установки агента аутентификации vGate. Кроме того, использование вышеупомянутой утилиты управления clacl.exe не позволяет повышать права пользователей без привилегий администратора учетных записей.

В результате дальнейшего тестирования по методу серого ящика была обнаружена мелкие недочёты, отраженные в составленном отчёте о проведении тестирования на проникновение, который был предоставлен ответственным за разработку лицам из ООО «Код Безопасности». Отдельно было отмечено, что все вышеперечисленные атаки провоцировали создание предупреждений в журнале аудита vGateR2, что позволяло отслеживать любую активность злоумышленника, кроме пассивного сбора информации при помощи анализатора трафика. На рисунке 8 показан пример события аудита.

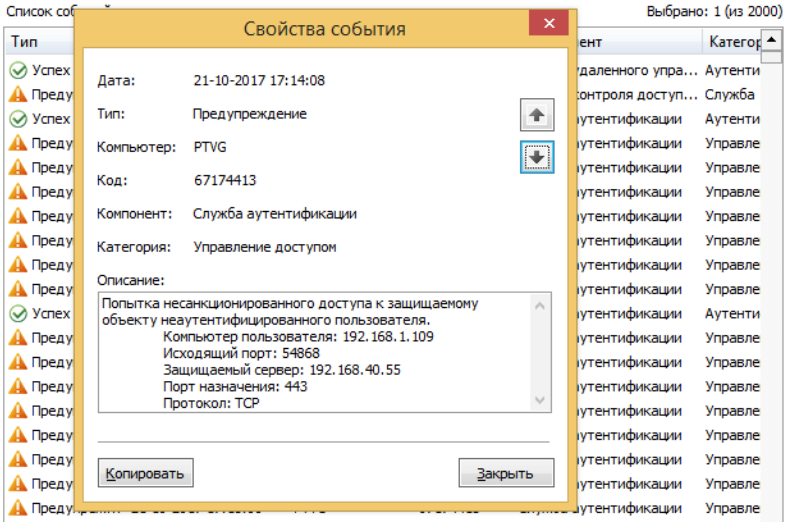


Рис. 8. Предупреждение о попытке перебора пароля от сервера ESXi

Заключение. В статье было рассмотрено проведение тестирования на проникновение с двух позиций: внешнего нарушителя, использующего возможности дистрибутива KaliLinuxи внутреннего нарушителя, располагающего ограниченными правами в системе. Приведена краткая методика проведения подобного тестирования и приведены некоторые примеры возможных атак.

В результате проведения исследования можно заключить, что тестирование на проникновение является важной частью обеспечения информационной безопасности и позволяет увидеть проблемы, которые могут оставаться скрытыми для специалистов в сфере информационной безопасности, но доступны для использования злоумышленниками.

СПИСОК ЛИТЕРАТУРЫ

1. Плешков А. С., Рудер Д.Д. Тестирование на проникновение как анализ защищенности компьютерных систем // Известия Алтайского государственного университета. – 2015. – №1. – С. 174-181.
2. Scarfone K., Souppaya M., Cody A., Orebaugh A., NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment. – USA, Gaithersburg. 09.2008. – 80 p. URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (дата обращения: 27.10.2017).
3. Богораз А. Г., Пескова О. Ю. Методика тестирования и оценки межсетевых экранов // Известия Южного федерального университета. Технические науки. – 2013. – №12. – С. 148-156.
4. Раздел «Документация vGate» [Электронный ресурс] // Официальный сайт ООО «Код Безопасности» [сайт]. URL: https://www.securitycode.ru/products/vgate/documentation/ (дата обращения: 27.10.2017).
5. Лещёв В. А. Технология тестирования программных модулей // Молодой ученый. – 2016. – №12. – С. 168-170.
6. Старцев С.С. К вопросу защиты беспроводных сетей на базе технологии Wi-Fi // Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2012. – Т. 10. – №1. – С. 63-72.
7. Key Reinstallation Attacks – Breaking WPA2 by forcing nonce reuse [Электронныйресурс] // Key Reinstallation Attacks [сайт]. URL: https://www.krackattacks.com (датаобращения: 27.10.2017).

УДК 004.93.12

ИДЕНТИФИКАЦИЯ ДВИЖУЩИХСЯ ОБЪЕКТОВ В ИНТЕЛЛЕКТУАЛЬНЫХ РАСПРЕДЕЛЕННЫХИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМАХ

Закасовская Елена Владимировна [1], Тарасов Валентин Сергеевич [1], Нютенко Сергей Игоревич [2]
[1] Дальневосточный региональный учебно-научный центр по проблемам информационной безопасности ДВФУ (ДВРУНЦ)
Россия, Владивосток, ул. Суханова, 8
[2]Дальневосточный федеральный университет (ДВФУ)
Россия, Владивосток, ул. Суханова, 8
e-mails: zakasovskaya.ev@dvfu.ru, tarasov_vse@students.dvfu.ru

Аннотация. В статье рассматривается задача распознавания образов для распределенной волоконно-оптической измерительной системы; при мониторинге движущихся объектов для распознавания образов целесообразен комплексный подход решения проблем обработки данных, который и был реализован в данной работе с помощью создания экспертной системы с применением нейронных сетей, которые были обучены и протестированы. Произведен сравнительный анализ полученных результатов с эталонными данными.

Ключевые слова: *экспертная система; нейронные сети; распределенные волоконно-оптические измерительные системы; распознавание образов; большие данные.*

IDENTIFICATION OF MOVING OBJECTS IN DISTRIBUTED INFORMATION-MEASURING SYSTEMS

Zakasovskaya Elena[1], Tarasov Valentin[1], Nyutenko Sergei[2]
[1]FarEastern Regional Science Center of Information Security Problems FEFU, (FERSC)
Russia, Vladivostok, Sukhanovastr., 8
[2]Far Eastern Federal University (FEFU)
Russia, Vladivostok, Sukhanovastr., 8
e-mails: zakasovskaya.ev@dvfu.ru, tarasov_vse@students.dvfu.ru

Abstract. The article reviews the problem of pattern recognition for a distributed fiber-optic measuring system; when monitoring moving objects for pattern recognition, an integrated approach to solving data processing problems is advisable, which was implemented in this work by creating an expert system using neural networks that have been trained and tested. A comparative analysis of the results obtained with the reference data is made.

Keywords: *expert system; neural networks; distributed fiber-optic measuring systems; pattern recognition; big data.*

Введение. Для мониторинга состояния периметра крупномасштабных объектов использование человеческого труда весьма неэффективно. Успехи в области технологии создания аппаратных средств и инженерного проектирования, в частности в сфере разработки технических средств охраны периметров и охранной сигнализации, привели к появлению различного рода технологий обеспечения безопасности, использующие:

– беспроводные сенсорные датчики;
– волоконно-оптические датчики (ВОД).

Существующий успех и большие перспективы развития информационно-измерительных систем (ИИС) в значительной мере связаны с тем, что сенсорные сети, построенные по одним и тем же принципам, могут применяться в совершенно различных областях человеческой деятельности [1]. Однако беспроводные датчики имеют ряд ограничений, оказывающие негативное влияние на обеспечения информационной безопасности при передачи данных внутри сети и за ее пределы.

Для достижения защищенной системы безопасность должна быть интегрирована в каждый аспект проектирования системы и в каждый ее компонент, так как любой слабозащищённый или вовсе незащищенный элемент, может стать местом атаки злоумышленника. При этом следует соблюдать компромисс между необходимыми функциональными возможностями и достаточным уровнем защищенности ИИС [2].

На сегодняшний день одним из перспективных направлений, относящихся к средствам мониторинга явлений, являются исследования в области волоконно-оптических измерительных систем (ВОИС). Волоконно-оптические элементы нечувствительны к электромагнитным помехам и способны работать в агрессивных средах. В связи с чем, использование распределённых волоконно-оптических измерительных сетей для охраны периметра в критических инфраструктурах представляется более эффективным по сравнению с системами, использующие беспроводные сенсорные сети (БСС).

В настоящее время процесс мониторинга состояния периметра с помощью распределённой измерительной системы не ограничивается одним обнаружением самого объекта, а требует оценки и анализа полученных данных с измерительных линий, регистрации и воспроизведения важнейших характеристик состояния объекта в реальном времени, передачи обработанной информации лицу, принимающему решения. Это новое понимание мониторинга как информационного мониторинга сейчас получило развитие и делает более ёмким его по содержанию [3].

Использование интеллектуальных распределенных волоконно-оптических измерительных систем (РВОИС), сопряжено с решением проблемы классификации поступающих данных об объектах и автоматического принятия на их основе в режиме реального времени решения о дальнейших действиях. Для решения данной проблемы весьма эффективно применение нейронных сетей.

Структура РВОИС, для которой разрабатывается экспертная система имеет сегментарный вид. Это обусловлено тем, что использование нейронных сетей для очень протяженной измерительной сети связано с определенными проблемами [4-7]:

– обучение такой сети требует длительного времени и больших вычислительных мощностей;
– поступающая информация с измерительных линий определяется не только воздействием физического поля контролируемого объекта, она зависит от множества других параметров и факторов;
– при контроле движущихся объектов изменчивость картины данных, полученной с измерительной сети, затрудняет, а в ряде случаев делает невозможным оперативное выделение признаков, по которым его можноклассифицировать.

Отдельный измерительный сегмент занимает малую площадь, чтобы разброс параметров измерительных линий и дефекты оптоволокна не вызывали существенного отклонения характеристик измерительных сегментов друг от друга.

Такая структура позволяет ограничиться обучением нейронной сети лишь для одного сегмента, что, очевидно, намного меньше времени обучения нейронной сети для несегментированной измерительной системы. Процесс распознавания образа в данном случае включает несколько стадий. Сначала по информации, полученной от измерительного сегмента, происходит быстрый поиск интересующих образов без учета местоположения воздействия (режим ожидания). Если обнаружены образы, требующие внимания, то на следующем шаге производится выделение измерительных сегментов, содержащих эти образы, определяется их расположение, а также другие характеристики, позволяющие отнести их к известному классу образов.

Таким образом, функционирование таких систем как ИРИИС будет складываться из выполнения следующих этапов:

1) Регистрация данных РВОИС и получение модели реального образа.

2) Сравнение модели реального образа с имеющимися образами в памяти экспертной системы и определение измерительного сегмента, в котором интересующий образ найден, с определением принадлежности данного образа к одному из известных классообразов.

3) Принятие решения и, при необходимости, выработка рекомендаций для проведения дальнейшего распознавания с поиском дополнительных признаков, характеризующих образ и его поведение в сегменте.

Основной функцией создаваемой экспертной системы является функция распознавания нарушителя либо беглеца и сообщения привилегированным пользователям о том, что необходимо выполнить определенные действия для решения проблемы. Структурно-функциональная модель представлена на Рисунке 1.

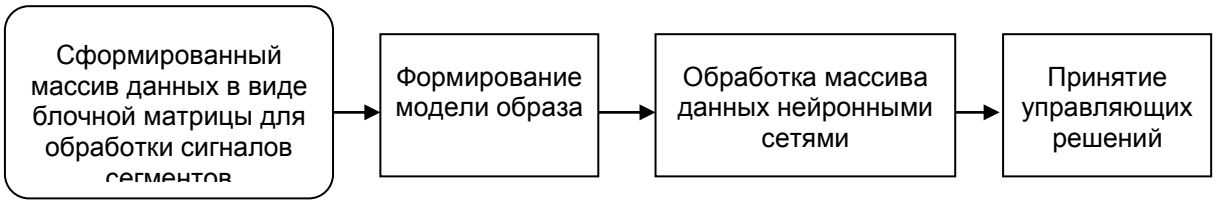


Рис. 1. Система обработки данных для распознавания образов

Для создания экспертной системы с помощью интерактивной среды для программирования MatlabR2016b был написан генератор данных, поступающих с измерительных линий. Он реализует 4 возможных исхода, представленных в Таблице 1.

Таблица 1

Обозначение класса	Направление движения	Масса, кг
Человек	На территорию объекта (нарушитель)	60-100
Человек	С территории объекта (беглец)	60-100
Катящийся	На территорию объекта (нарушитель)	200-400
Катящийся	С территории объекта (беглец)	200-400

Измерительная сеть в генераторе была представлена параллельно уложенными измерительными линиями в количестве 10 штук на расстоянии 40 см друг от друга. Масса и направление движения для каждого класса выбирались случайным образом из указанного диапазона. Как видно, генератор рассматривает простые случаи: классов всего 2, а направление условно разделяется на «вперед» и «назад». Расширение перечня классов с соответствующими им диапазонами массы и возможных траекторий требует наличия сложных систем, симулирующих движение человека.

Исследования проводились на простых случаях, чтобы в случае успеха можно было в дальнейшем глубже рассмотреть решаемые задачи [8]. В данном генераторе для большей правдоподобности шага человека определялось какой частью стопы было оказано воздействие. В зависимости от этого менялась амплитуда воздействия. Такие параметры как ширина шага, длина стопы, масса, начальное положение хода, время активности выбирались случайным образом из предусмотренных диапазонов.

Генератор представленный в данной работе создает выборку данных, поступающих с измерительной сети, в размере 10200 экземпляров. Пример сгенерированных данных представлен на Рисунке 2.

Одна из главных проблем при работе, распределенной волоконно-оптической измерительной сети – огромный поток данных, который нужно обрабатывать. В связи с необходимостью обрабатывать огромные потоки данных, целесообразно сжимать данные без существенной потери в них информативности. Для этого необходимо выделить характерные признаки исследуемого объекта из картины воздействий на измерительную сеть во время ее опроса.

Перед тем, как выделять признаки, входные данные должны пройти этап предобработки. Для этого применяется скользящее среднее - широко используемый индикатор в техническом анализе, который помогает сгладить сигнал, отфильтровывая "шум" от случайных колебаний.

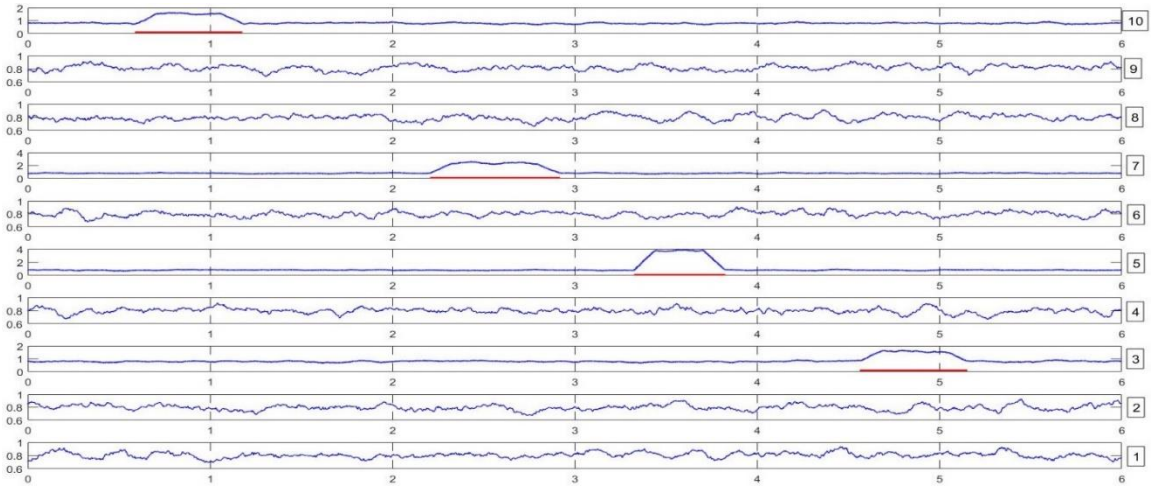


Рис 2. Шагающий (беглец)

Для данной задачи использовалось простое скользящее среднее[9]:

$$SMA_t = \frac{1}{n}\sum_{i=0}^{n-1} p_{t-i}, \quad (1)$$

где SMA_t -значение скользящего среднего в точке *t*, *n* – количество значений исходной функции для расчета скользящего среднего (сглаживающий интервал или период), чем шире сглаживающий интервал, тем более плавный график функции, p_{t-i}- значение исходной функции в точке *t-1*.

Выделение набора характерных признаков осуществляется для формирования из них массива признаков, который подается на вход нейронной сети, при определении основных параметров идентифицируемого движущегося объекта. Полный набор признаков представлен в Таблице 2.

Таблица 2

№	Признаки
1	Продолжительность инцидента
2	Число активныхизмерительных линий
3	Сумма числа воздействий по всем линиям за время инцидента
4	Среднеквадратичное отклонение числа воздействийпо линиям
5	Среднеарифметическое значение амплитуд воздействийпо всем линиям
6	Среднеквадратичное значение амплитуд воздействийпо всем линиям
7	Средняя периодичностьвоздействий
8	Среднеквадратичное отклонение периодичностивоздействий
9	Непрерывность воздействия на измерительную линию
10	Параллельность воздействия на измерительную линию
11	Одновременностьвоздействий на всю измерительную сеть
12	Направление
13	Взвешенный центр массы положения (прямым временем)
14	Взвешенный центр массы положения (обратным временем)
15	Максимальное воздействие на измерительную сеть во время инцидента

Для каждой задачи (распознавание класса, определение направления, определение массы) обучалась отдельная нейронная сеть. На вход каждой подавалась раннее сгенерированная выборка из 10000 векторов. Для проверки созданных сетей использовались 200 векторов, не входящие в обучающую выборку. Во всех случаях для обучения используется метод Левенберга-Марквардта. Этот метод является наиболее широко используемым алгоритмом оптимизации. Он превосходит простой алгоритм градиентного спуска и другие методы. Его можно рассматривать как сочетание наискорейшего спуска и метода Гаусса-Ньютона. Если текущее решение далеко от правильного, алгоритм ведет себя как метод наискорейшего спуска: медленно, но гарантированно сходится. Если текущее решение близко к правильному решению, становится методом Гаусса-Ньютона.

На вход вводится матрица размерности 15x10000. В качестве эталонов использовались векторы размерность 10000, содержащие 0 и 1, означающие шагающий и катящийся, либо нарушитель и беглец для сетей определения класса и направления соответственно. В качестве сетей распознавания класса и направления были использованы двухслойные feed-forward network с hidden neurons и линейными выходными нейронами (fitnet). Архитектура сетей для задач определения класса и направления представлена на Рисунке 3. Такая сеть может при необходимом количестве нейронов в скрытом слое соответствовать достаточно хорошо многомерным задачам отображения [10].

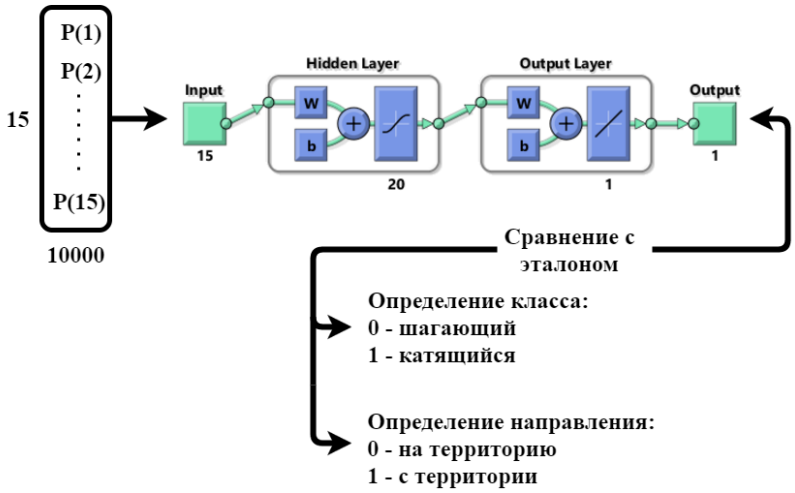
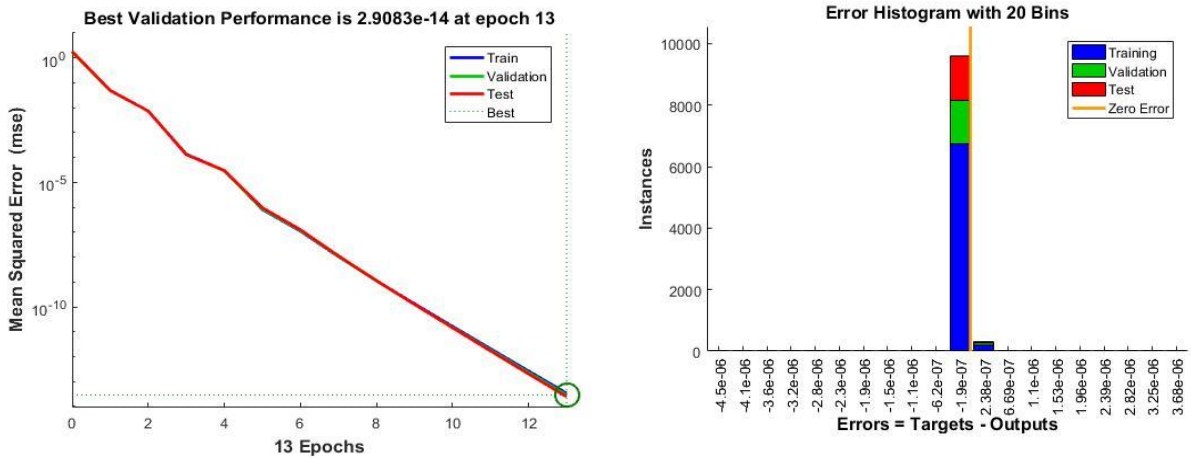


Рис. 3. Архитектура сетей для задач определения класса и направления

После определения архитектуры нейронной сети и выставления тренировочных параметров начинает процесс обучения, в ходе которого определяются и корректируются значения весовых коэффициентов, которые бы минимизировали ошибку на выходе нейронной сети. Обучение продолжается до тех пор, пока график проверки (линия validation) идет на спад. В качестве функции выполнения использовалось Means Squared Error – среднеквадратичное отклонение (ошибка). Линия проверки (a) игистограмма ошибок (b) представлена на Рисунке 4.



(a) (b)

Рис. 4. – Среднеквадратичное отклонение для сети определения класса и гистограмма ошибок сети определения класса

В настоящем исследовании 70% от общего объема данных выбраны случайным образом с целью обучения нейронной сети, 15% - для измерения сетевого обобщения, (обучение прекращается, когда обобщение перестает улучшаться); остальные 15% - для проверки работы обученной сети. В ходе тестирования созданных сетей ошибка по обучающему множеству для определения класса составила 0%, ошибка по обучающему множеству для определения направления составила 0%.

На вход подается та же выборка, а в качестве эталонов выступают конкретные массы для каждого вектора. В ходе тестирования созданной сети ошибка по обучающему множеству составила 12.24%, а максимальное отклонение от эталонного значения составляло 34.3392%. Критерий минимума среднеквадратичной ошибки стремится к равномерному распределению абсолютной ошибки и по всем векторам обучающей выборки и это приводит к критическим значениям относительной ошибки для объектов с малой массой. Для решения этой проблемы была проведена

нормализация эталонных выходов посредством извлечения кубического корня. Во время работы с нейронной сетью будет необходимо обратно масштабировать, т.е. возводить в куб. Такая сеть во время тестов показала себя намного лучше. Ошибка по обучающему множеству составила 2.2478%, а максимальное отклонение значения составило 10.7388%.

Таким образом были обучены все необходимые нейронные сети.

Заключение.Построенные сети были протестированы и почти со 100 процентной точностью определяют класс и направление, а отклонение при определении массы от фактической массы может составлять до 10.7%, что является хорошим результатом. Предобработка данных и их преобразование с помощью выделения характерных признаков позволяет значительно увеличить скорость обработки нейронными сетями и позволяет решать задачу распознавания движущихся объектов в зоне мониторинга с высокой точностью.

СПИСОК ЛИТЕРАТУРЫ

1. Выборнова, А. И. Исследование характеристик трафика в беспроводных сенсорных сетях: дис. … канд. техн. наук / А. И. Выборнова. – СПбГУТ, СПб.: 2014. – 183 с.
2. Закасовская Е.В., Тарасов В.С. Проблемы информационной безопасности в распределенных информационно-измерительных системах. Вкн.: Юбилейная XV Санкт-Петербургская международной науч.-прак. конф. «Региональная информатика (РИ-2016)», Санкт-Петербург, 2016. Санкт-Петербург: СПБГУ, 2016.
3. Кульчин, Ю.Н. Распознавание динамического объекта по восстановленному сигналу волоконно-оптической измерительной системы / Ю.Н. Кульчин, А.Ю. Ким // Материалы НТК «Молодежь и научно-технический прогресс», ДВГТУ, г. Владивосток, 2004. –111 с.
4. Кульчин, Ю.Н. Распределенные волоконно-оптические измерительные системы / Ю.Н. Кульчин – М: Физматлит, 2001. – 272с.
5. Кульчин, Ю.Н. Распознавание динамического объекта по восстановленному сигналу волоконно-оптической измерительной системы / Ю.Н. Кульчин, А.Ю. Ким // Материалы НТК «Молодежь и научно-технический прогресс», ДВГТУ, г. Владивосток, 2004. –111 с.
6. Саймон, Х. Нейронные сети: полный курс. (Neural Networks) – 2-е изд., исправленное / Х. Саймон. – М. : «Вильямс», 2006. – 1103 с.
7. 1. Денисов, И. В. Архитектуры систем искусственного интеллекта. / И.В. Денисов – Вл-к.: Изд-во МГУ им. Г.И. Невельского, 2004. – 231с.
8. Ким, А. Ю. Распознавание динамических образов интеллектуальной распределенной информационно-измерительной системы сегментарного типа: дис. … канд. техн. наук / А. Ю. Ким. – ИАПУ, 2014. – 183 с.
9. Скользящая средняя [Электронный ресурс] – Электрон. дан. – Режим доступа: https://ru.wikipedia.org/wiki/Скользящая_средняя.
10. Haritonova, P.L. On the modeling of artifical neural networks / P.L. Haritonova // International Scientific and Practical Conference «WORLD SCIENCE». – 2016. – p. 47-55.

УДК 004.04+658.5

МОДЕЛИРОВАНИЕ СЛОЖНЫХ МАШИНОСТРОИТЕЛЬНЫХ ИЗДЕЛИЙ В ХОДЕ ПРОИЗВОДСТВЕННЫХ ИСПЫТАНИЙ

Первухина Елена Львовна, ОсиповКонстантин Николаевич, Голикова Виктория
Севастопольский государственный университет
Россия, Севастополь, ул. Университетская, 33
e-mails: pervukhina14 @mail.ru, assistenttmm@mail.ru,golikova.victoria@gmail.com

Аннотация. Ранее предложенный авторами метод моделирования сложных машиностроительных изделий в ходе их производственных испытаний анализируется в контексте теории квалиметрии моделей сложных объектов.

Ключевые слова: *моделирование; квалиметрия моделей;сложные машиностроительные изделия; производственные испытания.*

MODELINGOF THE COMPLEX MACHINES DURING THEIR ACCEPTANCE TESTING

Pervukhina Elena, Osipov Konstantin, Golikova Victoria
Sevastopol State University, Russia, Sevastopol, Universitetskay str., 33
e-mails: pervukhina14 @mail.ru, assistenttmm@mail.ru,golikova.victoria@gmail.com

Abstract. The method of complex machine modeling, which is previously proposed by the authors, is analyzed in the context of the model qualimetry theory.

Keywords: *modeling; model qualimetry; complex machine-building products; production tests.*

Введение. В связи с ужесточением требований к качеству, в том числе надежности, современных сложных машиностроительных изделий, расширением номенклатуры технических операций, усложнением и ростом разнообразия их конструктивных элементов и различий в условиях эксплуатации, задача совершенствования методов оценки технического состояния и контроля качества в ходе стендовых приемосдаточных испытаний перед сдачей в эксплуатацию продолжает оставаться актуальной, несмотря на появление автоматизированных стендов со встроенным программным обеспечением (ПО). Как правило, используемые традиционные методы оценки состояния изделий не позволяют оперативно определять скрытые производственные дефекты и

неисправности в течение ограниченного времени испытаний по ограниченному числу измеряемых параметров, особенно при стремлении производителей снизить расходы на испытания. Достижение требуемой для повышения конкурентоспособности продукции отечественного машиностроения достоверности и точности результатов испытаний при снижении расходов на них требует новых методов оценки технического состояния.

В научно-технической литературе последних лет присутствуют примеры методов и алгоритмов оценки состояния сложных машиностроительных изделий [1, 2]. Однако большинство из них уникально и не может быть использовано в массовом и серийном производстве, в том числе, из-за большой сложности предлагаемых моделей и, как следствие, необходимости измерять значительное число параметров и обрабатывать большой объем информации, что снижает точность и достоверность результатов испытаний и увеличивает их стоимость [3]. Операторам испытаний представляется информация только о состояниях отдельных параметров испытуемых изделий. Интегральную оценку их состояния и принятие решений относительно их годности к эксплуатации до сих пор должны выполнять квалифицированные операторы.

Цель работы. Целью работы является анализ ранее предложенного авторами метода оценки технического состояния современных машиностроительных изделий в ходе производственных (приемосдаточных, контрольных) испытаний как основы перспективных программ испытаний в контексте развиваемой в последнее время группой российских ученых теории квалиметрии моделей сложных объектов и выбор направлений его развития.

Особенности производственных испытаний сложных машиностроительных изделий и задачи их моделирования. Под сложными машиностроительными изделиями понимаются машины и механизмы сложной структуры, состоящие из большого числа конструктивно отличающихся узлов и элементов с различными принципами и условиями функционирования, рабочими процессами различной физической природы, с большим числом связей, аналитическое описание которых невозможно. Технологический процесс испытаний, представляя элемент системы управления, является этапом получения первичной информации при контроле качества. В ходе производственных (приемосдаточных, контрольных) испытаний происходит приработка деталей, т.е. интенсивное изменение микрогеометрии сопрягаемых поверхностей деталей в подвижных кинематических парах, проверяется работа систем смазки, питания и охлаждения. В предположении отбраковки до начала сборочного процесса бракованных деталей на стадии испытаний определяют качество сборки, проверяют соответствие технических характеристик изделий ГОСТ Р или ТУ и принимают решения об их годности к эксплуатации. Эмпирическая информация о текущих состояниях испытуемых изделий имеет вид последовательных значений диагностических параметров; отражающих рабочие процессы изделий в зависимости от условий функционирования; управляющих воздействий; характера обработки, передачи и хранения данных [4].

Полное математическое описание подобных объектов является трудной научной задачей. С точки зрения концепции создания интеллектуальных информационных технологий мониторинга [5-7], для комплексного моделирования сложных технических систем и объектов нужно учитывать: размерность их характеристик, многофункциональность, нелинейность и непредсказуемость поведения, его детерминированный и стохастичный характер, отсутствие полной информации об объекте в целом. Однако моделирование не является основной целью анализа измерительной информации. В общем случае, она заключается в получении обобщенных оценок совокупности параметров, значения которых подтверждают готовность изделия к эксплуатации либо указывают на деталь и вид дефекта, либо обеспечивают прогноз состояния с заданной точностью и интервалом прогноза и т.п. [8].

Моделирование представляет только этап исследования при управлении испытаниями или решения другой задачи, предполагающей оценку и прогнозирование технического состояния испытуемых изделий и динамику их функционирования. Модели должны отражать исследуемые свойства машин, полное отображение всех технических свойств не является обязательным. По определению работы [6], под результативностью моделирования понимается способность моделей давать конкретный целевой эффект. Это утверждение дает основание не добиваться полного, всеобъемлющего описания сложных объектов.

В научной литературе последних лет появились работы, предлагающие использовать статистические методы обработки измерительной информации, а также моделирования и анализа изменяющихся показателей машин для отслеживания динамики их технического состояния. Это направление параметрической диагностики в отдельных работах называют тренд-анализом [9, 10]. Оно предполагает систематический контроль технического состояния и уровня надежности эксплуатируемого множества однотипных машин с учетом особенностей их применения, в том числе на основе статистических данных, для определения тенденций изменения значений параметров машин и выявления их возможных отклонений от нормальных значений. Главным недостатком этих работ является контроль изменения скалярных величин – отдельных диагностических показателей изделий, а также использование традиционных статистических методов и критериев, которые могут дать ошибочные результаты в случае изменения наблюдаемых случайных величин,

коррелированных между собой. Поэтому тренд-анализ дополняет, а не заменяет существующие методики анализа и не может без учета всего множества диагностических параметров дать полную и достоверную картину наличия или развития неисправностей или дефектов.

Предлагаемый подход к моделированию. Для решения конкретных задач испытаний, как показано в работах авторов [4, 11], моделирование даже конструктивно сложных машин и механизмов в условиях неполной и нечеткой априорной информации об их техническом состоянии возможно современными методами многомерного статистического анализа с построением причинно-следственных зависимостей между диагностическими и структурными параметрами, отражающих динамику состояния изделий. Последние напрямую отражают техническое состояние изделий и качество сборки, (величина зазоров в сопряжениях, качество уплотнений, натяжение в резьбовых соединениях и т.д.), однако их измерение после сборки невозможно.

На первом этапе моделирования определяются наиболее информативные с точки зрения целей испытаний параметры испытуемых изделий. Под информативностью параметра понимается степень снижения неопределенности знаний о техническом состоянии испытуемых изделий после использования информации о его значениях по результатам испытаний.

Снизить расходы на испытания без снижения достоверности и точности решений, принимаемых по результатам испытаний обработки информации, можно, минимизируя множество контролируемых параметров и точек съема информации. Это особенно актуально, когда наиболее информативные параметры не поддаются измерению либо соответствующие технические возможности их измерения сдерживаются экономическими факторами.

Процесс испытаний может быть описан следующей совокупностью характеристик: {X, Y, U, W, S, **ξ**, V, MSt,T, Rst,T, RΣt,T}, где X={x1,…xn} – ненаблюдаемые параметры, Y={y1,…ym} – наблюдаемые показатели испытуемого изделия, U={u1,…up} – характеристики условий внешней среды; W={w1,… wq} – неконтролируемые действующие возмущения; S – множество точек съема информации; V – вектор движения точек съема информации (постоянное их местонахождение – частный случай); MSt,T $\in M$ – математическая модель, связывающая информативные параметры на основе наблюдаемых данных; RS – частное решение, принимаемое по MS; RΣ – окончательное решение на основе уточненной модели; t, T – время наблюдения и время принятия решения о состоянии изделия, его параметрах и характеристиках; **ξ** – способы представления информации.

Существуют разные классические метрики для выбора информативности параметров и проверки качества моделей [6]. Мы предлагаем использовать для этой цели информационный критерий, известный в литературе как дивергенция, или информационное расхождение Кульбака-Лейблера. Выбор информативных параметров и точек съема информации удобно проводить на основе информационного критерия путем определения множества признаков, свойства которых позволяют максимизировать различия между состояниями испытуемого изделия [12].

Оператор испытаний получает измерительную информацию о значениях параметра в виде k-мерного вектора $y_q = (y_1 \dots y_k)$, $q = 1 \cdots m$, где k – число точек съема информации, и вектор измерений характеризует состояние ξ_i из конечного множества состояний изделия. Принимается допущение, что априорные вероятности каждого состояния одинаковы, т.е. вектор y_q может с равной вероятностью относиться как к одному, так и к другому состоянию; $p_i(y_q)$ – плотность распределения для вектора y_q при условии, что он передает состояние ξ_i.

Определяются инвариантные свойства возможных состояний, которые используются для понижения размерности вектора измерений. Элементы вектора (множества) выбираются на основе значений информационного критерия, выступающего в качестве меры расстояния между различными состояниями испытуемого изделия; оценивается эффективность разделения этих состояний. Выбираются элементы, которым соответствуют наибольшие значения информационного критерия, т.к. они заключают в себе максимум различающей информации. Элементы, вклад которых в информационный критерий невелик, исключаются из рассмотрения.

Задача понижения размерности вектора $y_q = (y_1 \dots y_k)$ решается определением матрицы, преобразующей исходный вектор в вектор с элементами, максимизирующими расстояние между состояниями. Информация, отличающая состояние ζ_1 от состояния ζ_2, рассчитывается с помощью

$$\ln\frac{p_2(y)}{p_1(y)}$$

логарифма отношения правдоподобия . При этом средняя различающая информация для состояния ζ_2 определяется выражением

$$I(2,1)=\int_y p_2(y)\ln\frac{p_2(y)}{p_1(y)}dy \ .$$

Информационное расхождение Кульбака-Лейблера

$$J(1,2)=I(1,2)+I(2,1)=\int_y\left[p_1(y)-p_2(y)\right]\ln\frac{p_1(y)}{p_2(y)}dy$$

представляет полную среднюю информацию для различения двух состояний изделия ζ_1 и ζ_2, характеризующихся плотностями распределения $p_1(y)$ и $p_2(y)$ [12].

Следующий этап моделирования изделий предполагает определение причинно-следственных зависимостей между параметрами. При анализе эмпирической информации, поступающей в виде случайных последовательных значений диагностических параметров; отражающих рабочие процессы изделий, определение таких зависимостей проводится с использованием статистических тестов, например, теста К. Грейнджера на каузальность (причинность) [4, 11]. Согласно тесту, переменная x_t является каузальной по отношению к переменной y_t (обозначается $x_t \rightarrow y_t$), если при прочих равных условиях значения y_t могут быть предсказаны по значениям x_t, измеренным ранее, с меньшей ошибкой, чем без их использования. Для проверки гипотезы « x_t не влияет на y_t » (где x_t, y_t – скалярные процессы) оценивается справедливость зависимости y_t от последовательности значений y_t и x_t. Тест позволяет однозначно выявить динамическое взаимодействие между диагностическими параметрами в виде направлений причинно-следственных связей и наряду с другими алгоритмами определяет выбор наиболее информативных параметров испытуемых изделий. При этом для исправных изделий изменение одного из параметров в одинаковых условиях испытаний должно сопровождаться изменением всех остальных.

Использование результатов моделирования для решения задач испытаний. На стадии приемосдаточных испытаний измеренные значения диагностических параметров представляют нестационарные случайные процессы даже при работе изделий на установившихся режимах. Для исправных изделий нестационарные случайные процессы изменения значений основных диагностических параметров связаны линейными комбинациями с коэффициентами, являющимися стационарными случайными величинами. Различие технических состояний отражается в изменении вероятностных характеристик случайных процессов изменения диагностических параметров. При дефектах или неисправностях значения диагностических параметров, как правило, отклоняются от номинальных значений. Стандартные характеристики функционирования изделий также отклоняются от номинальных, происходит изменение статистических связей между параметрами. В этих случаях зависимости между нестационарными процессами изменения диагностических параметров теряют стационарный характер, меняются значения коэффициентов зависимостей. Такие ситуации отличаются от тех, когда изменения вызваны только сменой режима работы испытуемых изделий. Показано [11], что для исправных изделий статистические зависимости между параметрами не нарушаются.

Математическое обеспечение автоматизированных испытаний при описанном подходе к обработке измерительной информации ориентировано на представление оператору испытаний новой информации об изменении причинно-следственных зависимостей между диагностическими параметрами изделий. Определение динамики коэффициентов этих зависимостей составляет основу многомерной модели развития свойств испытуемых изделий, проверка стабильности зависимостей – основу информационной технологии для оперативной оценки их состояния.

На следующем этапе анализа проверяем свойства моделей: устойчивость, чувствительность, наблюдаемость, робастность. Для проверки гипотезы об адекватности модели измерительной информации используются статистические тесты следа, максимального собственного числа и т.д. Несмотря на многомерность, при ограниченном числе параметров модели просты для машинной реализации и интерпретации [13]. Модели могут быть дополнены детерминированными моделями, в

том числе построенными по результатам спектрального анализа, что особенно актуально при испытаниях сложных машин на неустановившихся режимах [11].

Для окончательной проверки оптимальности полученных оценок параметров испытуемых изделий вновь используется информационное расхождение Кульбака [12], согласно которому оптимальной считается оценка, параметры распределения которой наиболее близки к параметрам распределения истинного вектора состояния изделия.

Заключение. Анализ ранее разработанного авторами метода оценки технического состояния современных машиностроительных изделий в ходе производственных (приемосдаточных, контрольных) испытаний находится в соответствии с развиваемой в последнее время группой российских ученых теории квалиметрии моделей сложных объектов и может стать основой перспективных программ испытаний.

Развитие метода связано с разработкой универсальной методологии испытаний на основе системного подхода к созданию математического обеспечения для интеллектуального организационно-технического комплекса испытаний машиностроительных изделий выделенного класса.

СПИСОК ЛИТЕРАТУРЫ

1. Павленко Е.А. Статистические методы диагностирования технического состояния автомобильных транспортных средств / Е.А. Павленко // Автомобильная промышленность. – 2009. – №7 – С 29 – 30.
2. Халиуллин Ф.Х., Особенности составления диагностической матрицы Байеса при безразборной диагностики двигателей внутреннего сгорания / Халиуллин Ф.Х., Ахметзянов И.Р. // Международный научно-исследовательский журнал, 2016. – № 5 (47).– С. 205-209
15. Макушин А.А. Имитационное моделирование ДВС в рамках автоматизированной системы испытаний / А.А. Макушин, Е.В. Зубков, В.С. Бахвалова // Сборка в машиностроении, приборостроении – №6. – 2009 г. – С. 52 – 56.
16. Pervukhina E. Improvement of the acceptance test procedure for the external combustion engine after assembly by using the relationship between diagnostic parameters / E. Pervukhina, K. Osipov, Y. Rapatskiy // Journal of Machinery Manufacture and Reliability, 2011. – Vol.40. – № 2, – P. 171-175.
17. Охтилев М.Ю. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов / М.Ю. Охтилев, Б.В. Соколов, Р.М. Юсупов. – М.: Наука, 2006, 410 с.
18. Соколов Б.В. Концептуальные основы оценивания и анализа качества моделей и полимодельных комплексов / Б.В. Соколов, Р.М. Юсупов // Теория систем и управления, 2004. – № 6. – С. 5-16.
19. Майданович О.В. Интеллектуальные технологии автоматизированного мониторинга сложных технических объектов / О.В. Майданович // Труды СПИИРАН, 2013. – Вып. 6(29). – Стр. 201-216.
20. МайдановичО.В. Перспективные направления развития информационных технологий мониторинга и управления состояниями сложных технических объектов в реальном масштабе времени / О.В. Майданович, М.Ю. Охтилев, Б.В. Соколов //InternationalJournal "InformationModelsandAnalyses", 2012. – Vol.1. – С.318-335.
21. Епифанов С.В., Выбор эффективных критериев тренда для применения в алгоритмах параметрической диагностики / С.В. Епифанов, Б.А. Щербань, Ю.В. Черкасов // Авиационно-космическая техника и технология, 2012. – № 8 (95). – С. 232-240.
22. Миська А.Р., Трендовый контроль режимных параметров дизель-генераторных установок / А.Р. Миська // Авиационно-космическая техника и технология, 2010. – № 7 (74). – С. 155-158.
23. Emmenegger, J.-F. Harmonic Analysis and Cointegration of Diagnostic Parameter Time Series of Motors / J.-F. Emmenegger, E. Pervukhina, V. Golikova // International Journal of Pure and Applied Mathematics, 2013. – Vol. 82. – №1. –, P. 143-161.
24. Первухина Е.Л. Использование информационной меры в процедурах оценки дискретных стохастических систем при неизвестных ковариациях шумов / Е.Л. Первухина // Известия РАЕН, серия МММИУ, 1999. – т.3. – №3. – С. 100-106.
25. Первухина Е.Л. Управление автоматизированными производственными испытаниями ДВС с использованием информационных технологий / Е.Л. Первухина, В.В. Голикова, К.Н. Осипов, И.С Тимофеев. // «Перспективные системы и задачи управления»: материалы XI Всеросс. научно-практ. конф. и VII молод. школы-семинара «Управление и обработка информации в техн. системах»; ЮФУ. – Ростов-на-Дону : Изд-во ЮФУ, Т. 2. – 2016. – с. 22-30.

УДК 004.056.53

ОРГАНИЗАЦИЯ ДРЕВОВИДНЫХ ХРАНИЛИЩ ДАННЫХ С УЧЁТОМ РАЗМЕЩЕНИЯ В НИХ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

Романова Юлия Николаевна, Янюшкин Константин Александрович
Государственный университет морского и речного флота им. адм. С.О. Макарова,
Россия, Санкт-Петербург, ул. Двинская, 5/7
e-mails: romanovaiuli@gmail.com, kayahidden@gmail.com

Аннотация. В статье рассматривается задача формирования блоков данных для вычисления дайджеста структурированных хранилищ информации большого размера, а также размещения сформированных электронных подписей в этих хранилищах. Описаны свойства предложенного подхода, который позволяет хранить подписи в виде древовидной структуры (с учетом порядка их формирования), которая позволяет последующее добавление данных и электронных подписей в хранилище.

Ключевые слова: *электронная подпись; структурированное хранилище; сплошное файловое хранилище; cryptoapi; потоки данных; дайджест; хэширование данных.*

DESIGN OF TREE-BASED SERIAL DATA STORAGES WITH INCLUDED DIGITAL SIGNATURES

Romanova Yuliya, Yanyushkin Konstantin
Admiral Makarov State University of Maritime and Inland Shipping

Russia, St. Petersburg, Dvinskaya str., 5/7
e-mails: romanovaiuli@gmail.com, kayahidden@gmail.com

Abstract. Thispaperprovidesoneofpossiblewaysofformingdatablob from big data storage with serial accessforhashingfunction to form digital signature. Also, we describe the way of storing digital signatures of data parts inside of these storages, which allow to keep tree structure of signatures sequences and add subsequent data to storage.

Keywords: *digitalsignature; structured storage; big data storage; cryptoapi; data stream; data hashing.*

На современных предприятиях водного транспорта вся циркулирующая в них информация представлена в виде документов. На сегодняшний день практически все документы создаются изначально в электронном виде и, несмотря на то, что многие из них попадают на печать и подпись, продолжая свою жизнь в бумажном виде, всё больше документов остаются и хранятся исключител+ьно в электронном виде, сохраняя при этом свою юридическую силу [1]. Согласно российскому законодательству, электронные документы, при соблюдении определённых законодательных норм, могут использоваться как для сообщения юридических и физических лиц с государственными органами, так и между собой. Ведение архива последовательности обмена данными, подписанными электронными подписями в сложных конфигурациях согласования документов в современной бизнес-логике, является не очевидной задачей с ростом скорости обработки и числа обрабатываемых документов [2-5]. Архив может быть представлен как последовательный поток данных (возможно, только с последовательным доступом), который разворачивается в древовидную структуру, похожую на структуру каталогов современных файловых систем [2].

Для внедрения подписи в последовательное хранилище рассмотрим его структуру. Структура хранилища с подписью имеет вид непрерывной битовой последовательности, хранящейся на физическом носителе [6, 7]. Корневое хранилище состоит из суб-хранилищ, и потоков данных. Каждое суб-хранилище имеет имя и свойства, а также, в свою очередь, само является хранилищем, тем самым обеспечивая древовидную структуру данных. Поток имеет имя и свойства и хранит в себе последовательность неформатированных данных. К имеющимся суб-хранилищам в корневое хранилище добавляется ещё одно, с зарезервированным именем DigitalSignatures, которое содержит потоки с подписями с именами signature_N, где N номер подписи. Потоки с подписями хранятся в той последовательности, в которой они были созданы. Подписываемые данные для хэширования собираются следующим образом:

1. Выбирается первый поток или первое хранилище (исключается хранилище с именем DigitalSignatures), который/которое содержится в корневом хранилище, к хэшируемым данным добавляется его имя;
2. Затем, если это хранилище, таким же образом рекурсивно обходится всё содержимое (потоки и субхранилища) этого хранилища;
3. Если это поток, то содержимое потока целиком добавляется к хэшируемым данным;
4. После обхода найденных потоков/хранилищ открывается хранилище DigitalSignatures, если оно существует. К хэшируемым данным добавляются все содержащиеся в нём потоки с контейнерами подписей в порядке следования без учёта имён этих потоков;
5. Собранный blob данных хэшируется, используя, например, реализованные отечественным ПО Крипто ПРО CSP (для *nix и Windows платформ) интерфейсные функции MS Crypto API, позволяющие частичную последовательную загрузку хэшируемых данных в оперативную память ЭВМ.

Процесс формирования подписи будет производится с использованием сертификата, который содержит открытый ключ электронной подписи, а также сведения о владельце сертификата и удостоверяющем центре, который его изготовил. Сертификат, используемый для подписания документа, должен быть установлен в локальное хранилище сертификатов или находится на съёмном защищённом носителе, откуда его может извлечь только используемый криптопровайдер. Оператору системы предлагается выбрать один из сертификатов хранилища. Выбранный сертификат открывается соответствующим ему криптопровайдером (если такого нет, то выдаётся ошибка). Сертификат проверяется на валидность, после чего, если он валиден, осуществляется попытка открыть по ссылке из сертификата контейнер с закрытым ключом, который должен соответствовать открытому ключу из сертификата. Оператор должен ввести PIN-код для контейнера, если это потребуется.

При проверке валидности сертификата происходит попытка построить цепочку доверия (цепочку подписанных сертификатов вплоть до корневого доверенного сертификата), в том числе с использованием загрузки из сети по указанному в сертификате адресу. В это же время происходит загрузка из сети списка отозванных сертификатов по адресу из сертификата, а также сверка с этим списком. Таймаут на эти операции установлен в зависимости от технических условий, а также

требованиями регуляторов к обязательности проверки списков отозванных сертификатов. Помимо сформированной подписи в контейнер с подписью добавляются все сертификаты цепочки доверия. Структура контейнера закодирована в формате ASN.1, сертификаты и подпись в него входящие — согласно CAdES — RFC5126. Этот контейнер и записывается в поток Signature_N. Процесс формирования подписи и содержимое контейнера (Signed Message в терминах PKCS#7) представлен на рис. 1.

В процессе проверки подписи для формирования цепочки доверия используются только сертификаты из контейнера подписи и локальных хранилищ. Никаких загрузок сертификатов и списков отзыва сертификатов не происходит, если иного не предусматривают особые требования законодательства к сфере применения метода.

Результатом проверки может быть три состояния:

1. Подпись верна, цепочка доверия построена и её корневой сертификат является доверенным;
2. Подпись верна, но нет доверия к сертификату. В этом случае отображаются подробности ошибок проверки;
3. Подпись не верна, сертификат в таком случае не проверяется. Отображаются подробности ошибок проверки.

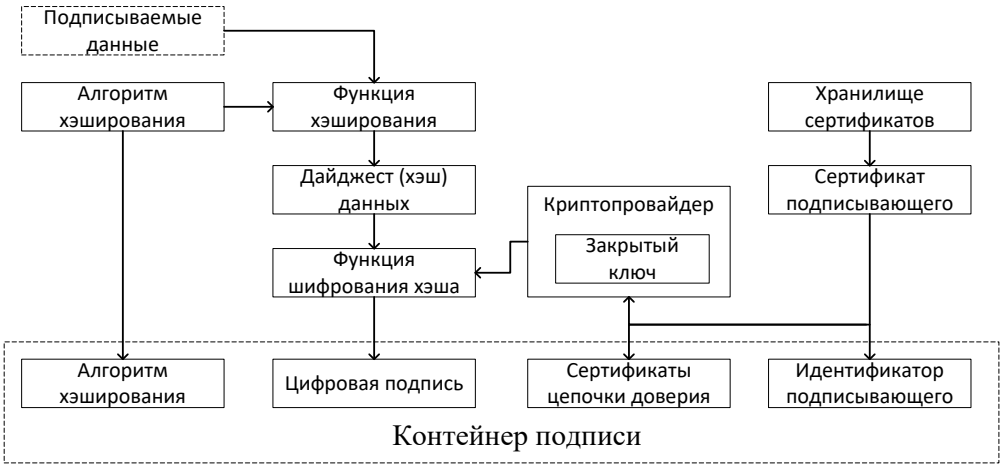


Рис. 1. Блок-схема процесса формирования подписи хранилища

Рассмотрим возможные преднамеренные или случайные изменения данных, расположенных в подписанном хранилище, а также последствия таких изменений [7-11]:

1. Смена порядка следования потоков/хранилищ приведёт к нарушению подписей документа;
2. Изменение содержимого любого потока приведёт к нарушению подписей документа;
3. Изменение имён потоков/хранилищ приведёт к нарушению подписей документа (кроме потоков хранилища DigitalSignatures, их имена не учитываются при подписании и могут быть изменены, это не повлияет ни на данные, ни на сами подписи);
4. Добавление любого нового потока/хранилища приведёт к нарушению подписей документа (кроме добавления нового, последующего потока в хранилище DigitalSignatures, он будет восприниматься как новая подпись);
5. Смена порядка следования потоков в хранилище DigitalSignatures приведёт к нарушению всех тех подписей, которые следуют за первым изменённым потоком, включая его;
6. Изменение любого потока в хранилище DigitalSignatures сделает соответствующую ему, а также все последующие подписи невалидными;
7. Удаление одного или нескольких последних потоков из хранилища DigitalSignatures не повлияет на работу, но все соответствующие потокам подписи документа будут удалены. Такое удаление будет невозможно отследить.

Заключение. Предложенная схема позволяет работать с последовательными хранилищами очень больших объёмов, содержащими древовидную структуру данных, которые могут быть подписаны последовательностью электронных подписей по мере заполнения.

СПИСОКЛИТЕРАТУРЫ

1. Нырков А.П. Автоматизированное управление транспортными системами / А. П. Нырков, С. С. Соколов, А. А. Шнуренко // СПб.: ГУМРФ имени адмирала С.О. Макарова, 2013. – 325 с.
2. Черняков А.В. Алгоритмы резервного копирования / Черняков А.В., Нырков А.П. // Материалы работы III научно–исследовательской конференции студентов и аспирантов факультета информационных технологий. «IT: ВЧЕРА, СЕГОДНЯ, ЗАВТРА – 2014» 19 декабря 2014 г. – СПб.: ГУМРФ имени адмирала С.О. Макарова, 2015. – С. 129–133.
3. Сабанов А. Г. Скиба В. Ю., Некоторые аспекты защиты электронного документооборота [Журнал] // Проблемы информационной безопасности. Компьютерные системы. - 2012 г. №2 стр. 42-45.
4. Bukharmetov M.R. Robust Method for Protecting Electronic Document on Waterway Transport with Steganographic Means by Embedding Digital Watermarks into Images / M. R. Bukharmetov, A. P. Nyrkov, S. S. Sokolov, S. G. Chernyi, V. N. Kuznetsov, D.

G. Mamunts // Proceedings of the 16-th Conference on Reliability and Statistics in Transportation and Communication, RelStat'2016, 19-22 October, Procedia Engineering 178, 2017. – С. 507 – 514. DOI: 10.1016/j.proeng.2017.01.097
5. Зима В.М. Молдовян А.А., Молдовян Н.А Безопасность глобальных сетевых технологий [Книга]. - СПБ. : БХВ-Петербург, 2003. - стр. 368. - ISBN: 5-94157-213-1.
6. GuntherothK. OptimizedC++: ProvenTechniquesforHeightenedPerformance [Книга]. - California (USA): O'ReillyMediaInc., 2016.
7. Summerfield M. Advanced Qt Programming: Creating Great Software with C++ and Qt 4 [Книга]. - London, England: Pearson Education (UK), 2016.
8. Куняев Н. Н. Демушкин А. С., Фабричнов А. Г., Конфиденциальное делопроизводство и защищенный электронный документооборот [Книга]. - Москва : Логос, 2011.
9. Мао В. Современная криптография. Теория и практика. [Книга]. - Москва : Вильямс, 2005.
10. Молдовян Н. А. Теоритический минимум и алгоритмы цифровой подписи [Книга]. - Санкт-Петербург: БХВ-Петербург, 2010.
11. Назаров С.В. Архитектура и проектирование программных систем: Монография [Электронный ресурс]. - М.: НИЦ Инфра-М, 2013 г.URL: http://www.znanium.com (дата обращения: январь 2017 г.).

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 327.8 : 061.1 ЕАЭС

ВОЗМОЖНОСТИ СМИ В ТРАНСФОРМАЦИИ ПОЛИТИЧЕСКОГО СОЗНАНИЯ ОБЩЕСТВ СТРАН ЕАЭС

Гайшун Александр Николаевич
«Красный пищевик»
Республика Беларусь, г. Бобруйск, ул. Бахарова,145
e-mail: alexandr.gaishun@gmail.com

Аннотация. Мировые средства массовой информации оказывают существенное влияние на процесс евразийской интеграции. Экономика, внутренняя и внешняя политика, этноконфессиональные отношения в странах ЕАЭС – это именно те сферы, где проявляется особенный интерес конкурирующих государств. Современная информационно-психологическая война ориентирована на дестабилизацию общества с целью демонтажа властных институтов.

Ключевые слова: *ЕАЭС; информационно-психологическая война; информационная безопасность.*

THE POTENTIAL OF THE MEDIA IN TRANSFORMATION OF POLITICAL CONSCIOUSNESS OF THE SOCIETIES OF THE EAEU

Gaishun Alexander
"Krasny pischevik", leading specialist of communications
Republic of Belarus, Bobruisk, St. Baharova, 145
e-mail: alexandr.gaishun@gmail.com

Abstract. The Global media have a significant impact on the process of Eurasian integration. Economy, domestic and foreign policy, ethno-religious relations in the countries of the EAEU – are exactly the areas, where special interest the competing States. Modern information-psychological war is aimed at destabilizing the society with the goal of dismantling government institutions.

Keywords: *EAEU; information-psychological war; information security.*

Сложные экономические и социально-политические процессы в современном мире оказывают колоссальное влияние на развитие постсоветских государств. Случившийся в 1991 году их «цивилизованный развод» по-прежнему провоцирует не только экономические, экологические трудности, но и обостряет политические, территориальные и этнические противоречия. Проект евразийской интеграции, как представляется, во многом направлен на мягкое, неконфликтное преодоление угрозы сталкивания бывших союзных республик в положение жестко контролируемых складывающимися ныне мировыми центрами силы региональных государств. Именно этим и объясняются масштабные операции информационного подавления ЕАЭС, реализуемые все более эффективно конкурирующими сторонами.

Сегодня можно вполне констатировать, что внешнеполитические успехи наиболее влиятельных стран определяются не только их экономической мощью и военным потенциалом, но и реализацией соответствующих программ, позволяющих поставить под контроль культурные и информационные процессы. Все эти усилия, в конечном итоге, подпадают под следующее определение современной информационно-психологической войны: это программа мер, направленных на дестабилизацию социума с целью свержения политического режима или изменения целевых политических установок правящей элиты, настроений граждан с использованием средств информационной борьбы.

Политические трансформации, начавшиеся в конце XX столетия и продолжающиеся в XXI - «цветные революции» в ряде постсоветских стран, а также смена властных режимов в Северной Африке и далее по «арабской дуге» свидетельствуют о том, что формирование и распространение по информационным каналам конкретной страны дезинформации или тенденциозной информации являются основным содержанием современной информационно-психологической войны.

Можно выделить несколько главных направлений информационных атак в отношении постсоветских государств, избравших стратегическим ориентиром евразийскую интеграцию. Первое.

Формирование чувства неприязни к идеям интеграции в Евразийском проекте у представителей политических элит, партий, движений, в целом среди населения в постсоветских странах. Второе. Критика социально-экономических курсов в России, Беларуси и Казахстане, Кыргызстане и Армении, ставящая под сомнение сами основы евразийской интеграции. Третье. Провоцирование раскола в группе стран – инициаторов создания Евразийского союза по социокультурным, конфессиональным признакам. Четвертое. Внедрение в сознание людей представления о том, что участие в интеграционном проекте приведет к потере государственного суверенитета странами, вступающими в ЕАЭС, ввиду неизбежного доминирования в нем Российской Федерации.

Мероприятия, направленные на манипулирование общественным сознанием в конкретной стране, особенно усиливаются в период проведения важнейших политических кампаний. Таковыми являются выборы главы государства, состава парламента, местных органов самоуправления.

В связи с этим, всем участникам евразийского проекта необходимо вполне осознать, что значение современных СМИ в реализации внешней и внутренней политики нельзя недооценивать. В Соединенных Штатах Америки, например, это хорошо понимают, что и подтверждает история взаимоотношений Белого дома и СМИ. Как отмечает в своем интересном исследовании Э.А. Иванян, «этим взаимоотношениям присуща динамика, они меняются, испытывая влияние требований времени, особенностей политического, экономического, социального, научно-технического, культурного и идеологического развития американского общества» [1, с.354]. Неизменным же остается главное – общие интересы Белого дома, олицетворяющего политическую и экономическую систему США и средств массовой информации, являющихся весьма действенным инструментом сохранения и упрочения этой системы.

Как представляется, далеко не в полной мере потенциал средств массовой информации каждой из стран-участниц евразийского проекта используется для подготовки необходимых аналитических материалов, отражающих наиболее злободневные вопросы их внутренней и внешней политики в контексте интеграционных процессов. Между тем, экономика, отношения с другими странами мира, социальная политика, этноконфессиональные отношения, - это те сферы, где всегда будут присутствовать попытки противодействия конкурирующим интеграционным проектам. Об этом безусловно свидетельствуют современные реалии.

Таким образом, проблема информационной безопасности оказывает существенное влияние на осуществление интеграционных проектов.

Возникающие противоречия между странами, участвующими в создании Евразийского союза, очень часто инспирируются государствами – конкурентами с помощью контролируемых в различных точках мира СМИ.

Одним из недавних, наиболее выразительных примеров такого рода действий стали белорусско-российские учения «Запад – 2017».

Тон общему хору задал сам командующий сухопутными войсками США в Европе генерал Бен Ходжес, увидевший в учениях «Запад-2017» образ «троянского коня» Кремля. Поддержали влиятельного генерала и европейские коллеги. Например, глава Минобороны Великобритании Майкл Фэллон заявил следующее: «Они (учения) призваны спровоцировать нас, они предназначены для проверки нашей обороны, и поэтому мы должны быть сильными» [2].

Совершенно понятно, что НАТО ныне главное средство контроля ведущей страны Запада над Европой. Однако настроения в ней совсем не те, какие были еще два-три года назад. Вот и существует великая потребность в формировании образа очень агрессивного врага. Менталитет же «осажденной крепости» в умах европейцев позволит США еще долгое время контролировать их политику.

К слову, в Европе многие понимают эти намерения. Например, немецкий обозреватель Тео Зоммер заметил, что «НАТО должно сделать все, чтобы обеспечивать безопасность своих восточных членов. Но альянс должен избегать того, чтобы соизмерять масштаб своих действий с их травмами и, тем более, истерией (президент Польши Дуда: «Мы готовимся к нападению»). К счастью, руководство альянса отреагировало взвешено: по словам генсека НАТО Столтенберга, «непосредственной угрозы странам НАТО не существует».

И вот продолжение, которое отражает нынешние представления значительной части политиков и экспертов (признаем, большинство не из столиц) государств Старой Европы: «Сегодня самое время не отдавать отношения с Россией на откуп одному только Североатлантическому альянсу… Политики должны осознать необходимость сотрудничества и искать возможности, например, в сфере контроля над вооружениями и, если смотреть дальше, в вопросе будущего мироустройства и места в нем России и Европы. И тут «Совет Россия – НАТО – не самое лучшее место для диалога: в плане больших перспектив его поле зрения слишком узкое» [3].

Безусловно, вся информационная возня вокруг белорусско-российских учений в иностранных СМИ – это очередная психологическая операция.

Заключение. Для государств ЕАЭС по-прежнему актуален вопрос сохранения национальной идентичности, ответ на который видится в совместном усилении интеграционных мотивов. Оптимизма добавляет недавняя общая историческая судьба, которая приводит к новым оценкам

периодов политического транзита и экономической разобщенности. Однако странам-участникам ЕАЭС необходимо в полной мере использовать все коммуникационные возможности для эффективного противодействия информационным операциям подавления.

СПИСОК ЛИТЕРАТУРЫ

1. Иванян Э.А. От Джорджа Вашингтона до Джорджа Буша. Белый дом и пресса. Москва: Издательство политической литературы, 1991
2. Учения «Запад -2017» призваны спровоцировать Запад – глава Минобороны Великобритании [Электронный ресурс] Режим доступа: www. ostro.org/ general/ society/ news/532415 Дата обращения: 11.09.2017
3. Зоммер, Тео. НАТО, тебе пора расслабиться! [Электронный ресурс] Режим доступа: www.inopressa.ru /article /19 Sep 2017/ zeit/ nato_ zapad 1. html Дата обращения: 20.09.2017

УДК 34.05

ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ В СЕТИ ИНТЕРНЕТ В ЕВРОПЕЙСКОМ СОЮЗЕ И РОССИЙСКОЙ ФЕДЕРАЦИИ

Долгошеин Пётр Сергеевич
Посольство России в Финляндии
e-mail: rlo.finland2@mvd.gov.ru

Аннотация. Статья посвящена исследованию методов противодействия распространению экстремизма и терроризма в сети Интернет в Европейском Союзе и Российской Федерации. Исследование выполнено на основе анализа бюллетеней, выпускаемых официальными источниками Европола и в Великобритании по обозначенному вопросу.

Ключевые слова: *Европол; полиция Великобритании; Российская Федерация; экстремизм; терроризм; метод; административно-правовое регулирование; участие граждан.*

COUNTERING EXTREMISM IN THE INTERNET NETWORK IN THE EUROPEAN UNION AND THE RUSSIAN FEDERATION

Dolgoshein Petr
Deputy representative of the Ministry of Internal Affairs of the Russian Federation
in Finland Republic
e-mail: rlo.finland2@mvd.gov.ru

Abstract. The article is devoted to the study tackling methods used in EU to counteract extremism and terrorism on the web. The study was performed on the basis of analysis bulletins issued by official sources in the United Kingdom and Europol, as indicated by the question

Keywords: *Europol; the UK police; Russian Federation; extremism; terrorism; method; administrative and legal regulation; citizen participation.*

Экстремизм не является статичным социально-правовым явлением, а динамично меняется вместе с обществом, используя в своих противоправных целях новейшие достижения науки и техники. Не является исключением и всемирная компьютерная сеть Интернет.

Государство, в лице правоохранительных структур, и население должны объединить усилия и находить новые формы и направления взаимодействия. Понимая всю опасность агрессивной информационной экспансии террористов и экстремистов, государства разрабатывают и принимают долгосрочные концепции программы, нацеленные на выявление и ограничение информационных потоков экстремистско-террористического толка, обнаружение лиц, причастных к этому. Однако, анализ подходов правоохранительных ведомств различных государств к решению указанного вопроса, показывает их неоднозначную эффективность.

Персонифицируя ответственность за конкретные действия, законодательством Российской Федерации, установлена административная ответственность за массовое распространение экстремистских материалов, включенных в опубликованный Федеральный список экстремистских материалов, а равно их производство либо хранение в целях массового распространения. Репост материалов из данного списка, является либо административным правонарушением, либо уголовным преступлением. Лицо, выложившее в сеть Интернет контент, содержащий сцены насилия, призывы к экстремизму или детскую порнографию, равно как и лицо, перепостившее данный контент, даже гневными замечаниями, находятся в равном положении с точки зрения уголовного правосудия. Можно констатировать, что Российское государство в лице правоохранительных органов, лишает граждан права высказывать свое отношение к ней, ограничивая тем самым Конституционные права на свободу поиска и использования информации (Ст. 24) и свободу мысли и слова (Ст. 29), если они не нарушают при этом прав и свобод иных граждан. Признавая запретительно-репрессивный характер подобных санкций государства, следует отметить, что при этом оно (государство) исключает из оборота контент, содержащий экстремистские материалы, минимизирует его оборот и тем самым

уменьшает количество пользователей, гипотетически способных случайно ознакомиться с данным контентом и впоследствии стать приверженцем и сторонником увиденного и услышанного.

Фактически на сегодняшний день в Российской Федерации наблюдается не всестороннее жизненно необходимое взаимодействие правоохранителей с населением в целях своевременного выявления экстремистского контента в сети Интернет с помощью законопослушных пользователей, а усиление карательной роли законодательства и «контрольно-сторожевых» функции силовых ведомств. В настоящее время единственно возможное действие для россиянина, не согласного с содержанием контента – молча выйти из него без каких-либо высказываний своей гражданской позиции и отношения (большей частью – негативного) к содержанию, а нередко и автору. Попытка оставить гневный комментарий по существу информации, влечет высокую вероятность пострадать самому, став уголовно-преследуемым субъектом распространения сведений экстремистского содержания. Угрозой подобного наказания Государство настраивает пользователей против себя и лишает правоприменителей потенциальной помощи огромного числа пользователей Интернета.

Иную доктрину противодействия экстремизму и терроризму в сети Интернет, демонстрируют правоохранительные органы Великобритании. Так Британское Национальное подразделение по борьбе с терроризмом в сфере Интернет (UK National Counter Terrorism Internet Referral Unit – CTIRU, далее – CTIRU) обратилось с призывом к населению сообщать о наличии в сети Интернет материалов, содержащих информацию экстремистского и террористического толка с помощью использования красной кнопки «СТОП», которую можно найти на веб-сайтах. После нажатия кнопки пользователем, интернет-провайдеры немедленно перенаправляют его на сайт www.gov.uk/report-terrorism~~pobj, на котором в анонимной форме просят ввести адрес веб-страницы, где пользователь увидел подозрительный материал. CTIRU исследует полученную от пользователей информацию, и в течение 36-часов обеспечивает удаление материала при его экстремистском характере. Размещение провайдером такого материала может привести к тому, что в отношении лица, опубликовавшего его, может быть проведено расследование в соответствии с Законом о терроризме 2006 года. Как правило, провайдеры незамедлительно реагируют на подобные обращения и удаляют подозрительный контент, что следует признать максимально прагматичным эффектом.

За период деятельности CTIRU с 2010 года по настоящее время, было изъято более 160 000 экстремистских и террористических материалов, значительная часть которых была выявлена именно с помощью общественности. В среднем в неделю удаляется более 1000 материалов. Активность участия населения в работе CTIRU постоянно увеличивается. Так в 2010 и 2011 г.г. население в данной программе не участвовало. В 2012 г.участвовало уже 1167 чел.; в 2013 г. – 923 чел.; в 2014 г. – 1462 чел.; в 2015 г. – 2995 чел.; Январь - март 2016 г. включительно – 785 чел.

Служба Европейской полиции решила использовать указанный опыт CTIRU. В апреле 2016 года Европол объединил свои усилия с Британским Национальным подразделением по борьбе с терроризмом в сфере Интернет для проведения 36-часовой операции по удалению в максимально быстрые сроки размещённого материала. В результате 1622 медиа контента и социальных медиа аккаунтов на 4-х языках, содержащих террористическую и жестокую экстремистскую пропаганду в 13 социальных медиа и онлайн провайдерах, были обработаны службой Европола.

Специализированным подразделением Европола по борьбе в сфере киберпреступности является IRU - Internet Referral Unit (далее – IRU). IRU начал свою деятельность в июле 2015 года. Основное направление деятельности – борьба с пропагандой терроризма и экстремизма в Интернете. С момента своего создания IRU оценило и обработало 11 000 сообщений от соответствующих провайдеров Интернет-услуг с 31 онлайн-платформы на 8 языках. 91,4% обработанных сообщений были удалены с платформ социальных сетей и поставщиков сетевых услуг.

Кроме того, IRU расширил свою деятельность с использованием открытого исходного кода и мониторинга сети Интернет для воспрепятствования деятельности нелегальных контрабандных сетей. Сотрудники IRU используют свои уникальные лингвистические возможности для обнаружения материалов, используемых Аль-Каидой или ISIS (Islamic State of Iraq and al-Sham – Исламское государство Ирака и Левана, террористическая организация, запрещённая в Российской Федерации).

Подводя итог, можно сделать вывод: при существовании потенциальной возможности использовать на территории России «красную кнопку», с помощью которой есть реальный шанс привлечь внимание властей к контенту, содержащему сцены насилия, призывы к экстремизму или материалы с детской порнографией – эта возможность была бы населением реализована.

СПИСОК ЛИТЕРАТУРЫ

1. Административный кодекс Российской Федерации [URL] http://www.consultant.ru/cons/cgi/online
2. Сайт Министерства юстиции [URL] http://minjust.ru/extremist-materials
3. Стратегия противодействия экстремизму в Российской Федерации до 2025 года [URL] http://www.scrf.gov.ru/security/State/document130/
4. Уголовный кодекс Российской Федерации URL] http://www.consultant.ru/document/cons_doc
5. Федеральный закон от 25 июля 2002 г. N 114-ФЗ "О противодействии экстремистской деятельности" (с изменениями и дополнениями) [URL Система ГАРАНТ: http://base.garant.ru/12127578/#ixzz4hvT0MmP7
6. http://news.met.police.uk/news/report-extremist-and-terrorist-material-online-160089
7. https://www.europol.europa.eu/newsroom/news/europol-internet-referral-unit-one-year

8. https:/www.europol.europa.eu/newsroom/news/europol-internet-referral-unit-one-year
9. https://www.gov.uk/government/speeches/baroness-shields-opening-speech-at-the-global-counter-terrorism-forum
10. http://www.independent.co.uk/news/uk/crime/junead-khan-luton-delivery-driver-found-guilty-of-preparing-for-uk-terror-attack-on-american-forces-a6963451.html
11. https://www.znak.com/2017-01-25/peskov_sluchay_s_chudnovec_ne_takoy_prostoy_s_nim_razbirayutsya

УДК 004.514.6

ДУХОВНО-НРАВСТВЕННЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИвентьевСергей Иванович
ООО «Юридическая Компания «ЮМАРК»
Россия, г. Казань, ул. Маршала Чуйкова, 9, офис 1
e-mail: sergei-zsk@mail.ru

Аннотация. В статье рассматривается информационная безопасность с точки зрения четвёртого и пятого поколений прав человека.Делается вывод, что информационные войны – не только уголовные, но и нравственные преступления. Обращается особое внимание духовно-нравственной безопасности человека, его души и духа.

Ключевые слова: *человек; душа и дух человека; права человека; права души и духа человека; информация; информационная безопасность; духовно-нравственная безопасность; информационные войны.*

SPIRITUALLY-MORAL ASPECTS OF INFORMATIVE SAFETY

IventievSergei
LLC «YUMARK Law Firm»
Russia, Kazan, st. Marshala Chuikova, 9, office 1
e-mail: sergei-zsk@mail.ru

Abstract. The article discusses information security from the point of view of the fourth and fifth generations of human rights. The conclusion is that the information war is not only criminal, but also a moral crime. Emphasizes moral and spiritual security of a person, his soul and spirit.

Keywords: *man, the soul and spirit of man, human rights, the rights of the soul and spirit of the person, information, information security, moral security, information warfare.*

Цель исследования – рассмотрение информационной безопасности с точки зрения духовно-нравственного аспекта и новых прав человека.

Задачи: раскрытие понятия «информация» и его производных; анализ научной, философской и иной литературы по теме исследования; выявление условий и причин информационных войн, раскрытие основ информационной безопасности, в том числе духовно-нравственной безопасности.

Используемые методы исследования: теоретические методы (изучение литературы по исследуемой теме, анализ, систематизация – классификация некоторых понятий, обобщение).

Введение.

Анализ становления прав человека показывает, что основу современной цивилизации до конца прошлого столетия составляли три поколения прав человека, которые были провозглашены в ходе буржуазных революций. К ним относят гражданские, политические, экономические и социальные права и свободы человека и гражданина. Как нами отмечалось, это права телесной сущности человека или права тела.

Российская юриспруденция по-новому взглянула на человека, его материальные и нематериальные блага. Человек стал рассматриваться не только как материальный носитель телесный прав, но и как духовно-нравственная личность, которой принадлежит определённый набор прав и свобод.

В конце XX века в Российской Федерации было открыто четвёртое поколение прав – духовно-нравственные права и свободы человека и гражданина, которые провозгласили и провозглашают духовные и нравственные ценности личности [1, с.183-185; 3, с.5-8].

К четвёртому поколению прав относятся право на жизнь, уважение духовного и нравственного достоинства человека, запрет пыток и бесчеловечного обращения, право на творчество, право выбора и свобода воли, свобода совести и вероисповедания, право на духовное образование и воспитание, право на духовное и нравственное совершенствование, право на благоприятную окружающую среду и другие права, которые вытекают из духовной и нравственной автономии человека.

В начале нашего столетия в России было провозглашено и введено в юридическую науку пятое поколение прав человека – Божественные права и свободы, основу которых составляют Любовь, Божественная информация и энергия [3, с.123-135].

К пятому поколению прав относят права: право на Любовь, Вера и любовь к Богу, единство с Творцом, право на рождение в Любви, право на обращение к Богу, право на информацию и

управление энергией, право на управление пространством-временем, материей, право на развитие энергетической мощи своей души и своих энергооболочек, право на Сотворчество и совершенствование окружающего мира, право на Божественное совершенствование, право на дары Бога, право человека на бессмертие и другие права, которые вытекают из Любви и Божественной энергии.

Четвёртое и пятое поколения прав человека направлены на защиту духовной сущности человека, его Души и Духа, которые бессмертны.

Четвёртое и пятое поколения прав человека – это права духа и души человека [3, с.183-185].

Благодаря вышеуказанным новым правам человека, можно по-новому взглянуть на различные духовно-нравственные и социально-культурные явления и события в жизни человека и общества.

Актуальным для общества является информационная безопасность с точки зрения четвёртого и пятого поколений прав человека.

Определение основных понятий.

Чтобы раскрыть исследуемый вопрос, нам необходимо привести имеющиеся общепринятые определения понятиям «информация», «безопасность», «информационная безопасность» и «информационные войны» и их производным.

Информация (от лат. informatio – осведомление, разъяснение, изложение, от лат. informare – придавать форму) – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [3, с.229; 7, с.125].

В юридической науке под информацией понимают «строительный материал», первооснову творимых, высказываемых или воспринимаемых людьми взглядов, суждений, оценок, мнений, сообщений, которые представляют собой личностно окрашенную информацию, отражающую чьи-либо позиции и интересы [7, с.228].

В статье 2 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» даётся правовое определение «информации», под которой понимаются сведения (сообщения, данные) независимо от формы их представления [14].

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз политического, экономического, социального, военного, техногенного, экологического, информационного и иного характера, предполагающее установление политической, экономической и социальной стабильности в государстве, безусловное исполнение законов и поддержание правопорядка, развитие международного сотрудничества на основе партнерства. Основными объектами безопасности являются: 1) интересы личности – конституционные права и свободы, личная безопасность, повышение качества и уровня жизни, физическое, духовное и интеллектуальное развитие; 2) интересы общества – упрочение демократии, достижение мира, поддержание общественного согласия, повышение созидательной активности населения и духовное возрождение; 3) интересы государства – конституционный строй, суверенитет и территориальная целостность [13, с.83].

Информационная безопасность – состояние сохранности информационных ресурсов и защищённости законных прав личности и общества в информационной сфере [12].

Информационная безопасность личности – состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда здоровью и (или) физическому, психическому, духовному, нравственному развитию человека [8].

Духовно-нравственная безопасность – обеспечение защиты духовной и нравственной сферы человека и общества, души и духа человека.

Информационная война (англ. Information war) – процесс противоборства человеческих общностей, направленный на достижение политических, экономических, военных или иных целей стратегического уровня, путём воздействия на гражданское население, власти и (или) вооружённые силы противостоящей стороны, посредством распространения специально отобранной и подготовленной информации, информационных материалов, и, противодействия таким воздействиям на собственную сторону; целенаправленные действия, предпринятые для достижения информационного превосходства путём нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем [10, с.73-80].

Обсуждение рассматриваемой темы.

Человек и гражданин имеют право на доступ к информации [2], что нашло своё отражение в международном праве и национальных законодательствах.

В соответствии со статьёй 33 Конституции Российской Федерации граждане имеют право на индивидуальное или совместное (коллективное) обращение в публичные (государственные и муниципальные) органы. Аналогичное положение также закреплено в международном праве (статьи 19 Всеобщей декларации прав человека и Международного пакта о гражданских и политических правах).

Согласно статье 8 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» каждый имеет право на доступ к информации [14].

Указанное право человека и гражданина на доступ к информации касается только политической и социально-культурной сфер, то есть рассматриваемое право является составной частью гражданских, политических, социальных и экономических прав человека.

В свою очередь, право человека на Божественную и духовно-нравственную информацию (энергию) входит в состав четвёртого и пятого поколений прав человека, то есть прав души и духа человека.

«В современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т.п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью» [4].

В приведённой классификации информационной сферы, к большому сожалению, отсутствуют понятия «духовно-нравственная информация» и «духовно-нравственная безопасность», что делает неясными в связи с этим некоторые понятия. Считаем, что данные понятия должны быть включены в эту классификацию отдельной группой.

Государства в основном обеспечивают информационно-техническую безопасность своих граждан. Сложнее дело обстоит с информационно-психологической и духовно-нравственной безопасностью человека, его души и духа (экстрасенсорное влияние, массовый гипноз, распространение деструктивных сект и антинравственной агитации, экстремистская вербовка через социальные сети, заговоры, магические ритуалы и другие энергоинформационные воздействия).

В настоящее время в Мире развёрнуты информационные войны, которые направлены не только на человека, но и его душу и дух, и представляют собой открытое враждебное посягательство на духовно-нравственную целостность человека, общество и государство.

Традиционно в науке к основным причинам правонарушений и преступлений относят экономические, институциональные и социально-культурные факторы, забывая о духовно-нравственном аспекте этих явлений.

Как правило, все преступления всегда носят нравственный характер, то есть все правовые преступления, определённые законом, являются нравственными преступлениями [5, с.122-125].

Информационные войны – это, прежде всего, нравственные преступления, которые духовно и нравственно разлагают человека, создают условия для его духовной деградации через антиморальную агитацию и порнографический и различный безнравственный материал, который подаётся через печатную продукцию, СМИ и социальные сети.

Системность рассматриваемого порока во многом обусловлена девальвацией системы духовно-нравственных ценностей.

Информационные войны всегда посягают на духовную и нравственную целостность личности, то есть противостоят четвёртому и пятому поколениям прав человека.

Идеологии информационных войн подвержена молодёжь. Через информационную идеологию формируются новые негативные идеалы и ценности, вербуются молодые люди в криминальные и террористические группировки.

Безусловно, что информационные войны представляют собой манипуляцию истиной, её искажением, а также увод человека от неё. Это связано, прежде всего, с тем, что на международном уровне отсутствует точное и не размытое правовое определение понятию «истина».

Через информационные войны доводится до людей корпоративные истины и различные государственные идеологии [6, с.167], которые часто направлены против человека.

Из-за не обращения государств, международных организаций на вопросы души и духа человека, информационные войны приобрели катастрофические масштабы.

Считаем, что наступило время человечеству немедленно заняться вплотную указанными архиважными вопросами, то есть принять меры по духовно-нравственному обновлению человеческого общества.

Как отмечает И.Х.Мамедов, «Совмещение духовного обновления и моральных традиций является серьезной научной проблемой. По этой причине, модернизация общества сам по себе бесконечный и сложный процесс» [11, с.339-341]. Чтобы решить данный вопрос, научное сообщество должно подготовить теоретический и практический материал для утверждения государственной идеологии в данной области.

Выводы и рекомендации.

Из-за размытых формулировок понятий основных элементов информационных войн, государство и общество окончательно не знают с чем или с кем имеют дело и не могут обеспечить адекватную духовно-нравственную защиту граждан.

Необходимо на международном и государственном уровне дать точные формулировки составным элементам информационных войн, чтобы определять адекватные и эффективные меры по противодействию распространения информационных войн и киберпреступлений, а также меры борьбы с указанными нравственными пороками.

Девальвация духовно-нравственных ценностей – основная причина нравственных и уголовных преступлений.

К большому сожалению, многие государства к мерам по обеспечению противодействия рассматриваемым нравственным порокам и уголовным преступлениям не относят возрождение и культивирование духовно-нравственных ценностей в обществе, а также публичное закрепление нравственных норм. Считаем, что необходимо обратить особое внимание на талантливую молодёжь, создав, с целью предотвращения появлению хакеров (англ. hacker, от to hack – обтёсывать, делать зарубку), необходимые условия работы на государство и общество. Надо доморощенных хакеров перевоспитывать и привлекать на благо общества. Важную роль в борьбе с информационными войнами играет просвещение граждан по вопросам миролюбивых религий, радикальных сект и религий. К большому сожалению, СМИ мало уделяет этому внимание, а занимается распространением культа потребления и насилия.

Государство мало обращает внимание вступлению подростков в преступные организованные сообщества, которые могут быть террористическими и националистическими группами.

К мерам по противодействию распространению идеологии экстремизма и терроризма, которые используют также информационные войны, среди молодёжи следует дополнительно отнести следующие меры. Считаем, что необходимо на законодательном уровне определить понятие «истина», чтобы не было возможности трактовать её с точки зрения экстремизма и радикализма, то есть выбить идеологическую составляющую экстремизма и любых информационных войн. Науке необходимо заняться изучением вопросами жизни после смерти, чтобы раскрыть суть экстремистской информационной идеологии. На международном уровне надо запретить использование секретными службами любых стран террористических группировок для выполнения своих задач.

Государству необходимо регулярно и на постоянной основе заниматься решением социально-экономических вопросов молодёжи (обучение и трудоустройство, предоставление жилья и земельных участков, обеспечение детей садиками и школами, лагерями для отдыха, центрами для детей и молодёжи и пр.).Обеспечение духовно-нравственной информационной безопасности граждан – это первостепенная задача любого государства.Безусловно, что особое внимание следует уделять мероприятиям, направленным на культивирование патриотизма у молодёжи, а также вопросам миграционной политики.

Заключение. Предусмотренный объём статьи не даёт возможность поподробнее рассмотреть исследуемую тему. Но несмотря на это, мы очертили основные пути решения вопросов информационной безопасности государства и общества, в том числе и духовно-нравственной безопасности человека.

Духовно-нравственное обновление человечества может начаться только с обращения мирового сообщества, всех государств на душу и дух человека.

СПИСОК ЛИТЕРАТУРЫ

1. Гузенко С.С.Что такое права души человека//Молодёжь и наука: материалы международной науч.-практ.конф. (26 мая 2017 г., г. Нижний Тагил) в 2 т. Т. 2/ Министерство образования и науки Российской Федерации, ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н.Ельцина», Нижнетагил. технол.ин-т (фил.). – Нижний Тагил: НТИ (филиал) УрФУ, 2017. – С.183-185.
2. Доступ к информации – права человека и интересы государства: материалы дискуссии в рамках семинара, проведенного архивным тренинговым центром при Европейском университете в Санкт- Петербурге. 16-17 марта 2000 года. – СПб.: М'АРТ, 2000. – 106 с.
3. Ивентьев С.И.Божественные и духовно-нравственные права и свободы человека: монография. – Новосибирск: ООО агентство «СИБПРИНТ», 2012. – 357с.
4. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009. – 456с.
5. Ивентьев С.И. Нравственные и правовые преступления Мира// Казанская наука. – 2010. – № 7. – С.122-125.
6. Ивентьев С.И.Истина. – Новосибирск: ООО «Агентство «СИБ-ПРИНТ», 2016. – 386с.
7. Конституционное право России: учебник/отв.ред.А.Н.Котов и М.И.Кукушкин. – М.: Норма: Инфра-М, 2010. – 544с.
8. Кунгаа М.М.Дефиниция понятия «информационная безопасность личности»//Экономика. Право. Менеджмент: сборник трудов молодых исследователей БГУ. – 2016. – № 2 (6).
9. Лукаш Ю.А.Российское законодательство. Толковый словарь для студентов. – М.: ГроссМедиа: РОСБУХ, 2008. – 448с.
10. Манойло А.В.Информационно-психологическая война: факторы, определяющие формат современного вооруженного конфликта. – Киев: Материалы V Международной научно-практической конференции «Информационные технологии и безопасность». – 2005. – № 8. – С.73-80.
11. Мамедов И.Х.Духовное обновление общества//Молодёжь – науке. 2016. Материалы молодёжных научно-практических конференций Псковского государственного университета по итогам научно-исследовательской работы в 2015/2016 учебном году. Т. VIII. – Псков: Псковский государственный университет, 2016. – С.339-341
12. Пилипенко В.Ф.Безопасность: теория, парадигма, концепция, культура. Словарь-справочник. 2-е изд., доп. и перераб. – М.: ПЕР СЭ-Пресс, 2005. – 192с.
13. Социологическая энциклопедия: в 2 т. – М.: Мысль, 2003. – 863с.
14. ФЗ «Об информации, информационных технологиях и о защите информации»//Российская газета, № 165, 29.07.2006.

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 371.1

ТЕОРИЯ ПРИНЯТИЯ РЕШЕНИЙ В ВОПРОСАХ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА

Большакова Людмила Валентиновна, Дашков Андрей Владимирович,
Яковлева Наталья Александровна
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, 1
e-mails: blv5505@mail.ru, andreyka070597@yandex.ru, kumirova@mail.ru

Аннотация. В докладерассмотрены методы решения задач, связанных с обеспечением экономической безопасности хозяйствующего субъекта. Решение происходит в условиях полной неопределенности или в условиях риска и обосновывается в рамках теории принятия статистических решений, в частности, с применением дерева решений.

Ключевые слова: *неопределенность; риск; статистическое решение; дерево решений.*

THE THEORY OF DECISION-MAKING IN MATTERS OF ECONOMIC SECURITY ENTITY

Bolshakova Lyudmila, Dashkov Andrey, Yakovleva Natalia
The St.-Petersburg University of the Ministry of Internal Affairs of Russia
Russia, St. Petersburg, Pilot Pilyutov st. 1
e-mails: blv5505@mail.ru, andreyka070597@yandex.ru, kumirova@mail.ru

Abstract. The paper considers methods for solving problems related to ensuring economic security of business entity. The decision takes place under conditions of uncertainty or under risk, and is grounded in the theory of making statistical decisions, in particular, with the use of a decision tree.

Keywords: *uncertainty; risk; statistical decision; a decision tree.*

Достаточно часто решение различных задач, относящихся к экономической безопасности хозяйствующего субъекта, происходит в условиях полной неопределенности или в условиях риска.

В этой ситуации, при выборе конкретных управленческих решений необходимо принимать во внимание как влияние отдельных неопределенных факторов, так и все последствия, возможные после принятия того или иного альтернативного решения.

Для выбора оптимального решения при условии наличия некоторых числовых характеристик, довольно успешно могут быть применены методы, которые разрабатываются и обосновываются в рамках теории принятия статистических решений. Условно эти методы могут быть разделены на три группы.

К первой группе можно отнести методы, использующие основные понятия теории игр, в частности, понятие платежной матрицы или матрицы решений.

Такие методы могут помочь руководителю в выборе одного из нескольких имеющихся вариантов. Они наиболее эффективны, когда лицо, принимающее решение, должно выявить, какая стратегия будет содействовать достижению целей, т.е. являться оптимальной в соответствии с некоторым принятым критерием.Вторая группа методов связана с прогнозированием. В этих методах используется как накопленный в прошлом опыт, так и текущие предположения о будущем с целью его определения и уточнения этого будущего. В последующем прогнозируемые результаты применяются как основа для планирования.

И, наконец, третья группа методов предполагает использование, так называемого дерева решений. Методы третьей группы применяются в задачах, в которых имеются многоэтапные (позиционные) решения, т.е. в тех, где присутствуют два (или более) последовательных множества решений, причем основаниями последующих решений являются результаты предыдущих, и/или два (или более) множества состояний среды (т.е. если появляется целая цепочка решений, исходящих одно из другого и которые соответствуют событиям, происходящим с некоторой вероятностью) [3].

Поясним применение дерева решений при исследовании конкретной проблемы, определив предварительно само это понятие и основные этапы применения соответствующего метода.

Дерево решений – это графическое отображение последовательности решений и состояний среды с указанием соответствующих вероятностей и выигрышей для любых комбинаций альтернатив и состояний среды.

Также под деревом решений можно понимать схематическое представление проблемы выбора. Ветви дерева решений представляют собой различные события (решения), а его вершины – ключевые состояния, в которых и возникает та самая необходимость выбор. Для того, чтобы определиться с конкретным решением, этот метод можно условно разделить на пять этапов, которые предполагают выполнение следующих действий:

1. Формулировка задачи. Для приведения описания задачи по принятию решения к поддающейся анализу форме необходимо выделить существенные и несущественные факторы, а также отбросить те, которые не относятся к проблеме. Нельзя забывать про выполнение следующих основных процедур: оценка возможности сбора информации для экспериментирования и реальных действий; составление перечня событий, которые с определенной вероятностью могут произойти; установление временного порядка расположения событий, в исходах которых содержится полезная и доступная информация, и тех последовательных действий, которые можно предпринять.

2. Построение самого дерева решений.

3. Оценка вероятностей состояний среды, т.е. сравнение шансов возникновения каждого отдельного события. Следует отметить, что указанные вероятности, как правило, определяются либо на основании имеющейся статистической информации, либо экспертным путем с применением метода экспертных оценок.

4. Установление выигрышей или проигрышей для каждой возможной комбинации альтернатив (действий) и состояний среды.

5. Решение задачи.

Допустим, например, что руководство некоторого хозяйствующего субъекта решает вопрос о выработке концепции экономической безопасности предприятия, которая включает комплекс подготовительных мероприятий.

При выработке концепции в распоряжении руководства имеются три возможных направления – три пакета действий: П1, П2, П3. Действенность каждого из пакетов зависит от определенного состояния экономической среды, например, от благоприятного или неблагоприятного. Состояние невозможно предсказать точно, однако существуют определенные компании, которые за конкретную сумму могут провести анализ возможного будущего состояния [4].

Выигрыши (или проигрыши) предприятия при разных состояниях среды и разных выборах направлений известны.

Ставится вопрос о том, какую стратегию лучше всего выбрать руководству предприятия. Задача существенно усложняется, если добавить исследование возможного прогноза состояния экономической среды, поручив его проведение некоторой фирме за определенную плату. Вероятности правильного прогноза фирмы также известны.

Какое решение следует принять руководству?

Для ответа на этот вопрос, на основании всех сведений можно построить дерево решений, где развитие событий происходит от корня дерева к конечным исходам, а расчет затрат или прибыли выполняется от конечных состояний к начальным.

Для предложенной выше задачи вначале строится от корня дерева две ветви, одна из которых предполагает, что руководство предприятия делает заказ фирме по проведению исследования, другая определяет отсутствие этого заказа. Далее каждая из этих ветвей продолжает деление на три ветви, соответствующие выбору П1, П2 и П3. И, наконец, в последнем разветвлении происходит разделение каждой ветви предыдущего этапа на две: с благоприятным или неблагоприятным состоянием экономической среды.

Необходимо отметить, что методы, связанные с применением дерева решений, используются крайне редко и не всегда правильно, хотя в сложных и неопределенных ситуациях их правильное применение часто приводит к получению оптимальных, адекватных действительности решений.

СПИСОК ЛИТЕРАТУРЫ

1. Моделирование рисковых ситуаций в экономике и бизнесе: Учеб. пособие / А.М. Дубров, Б.А. Лагоша, Е.Ю. Хрусталев, Т.П. Барановская; Под ред. Б.А. Лагоши. – 2-е изд., перераб. И доп. – М.:Финансы и статистика, 2003. – 224 с.
2. Орлов А. И. Теория принятия решений – Экзамен, 2005. 656 с.
3. Вилков В.Б., Большакова Л.В., Черных А.К., Яковлева Н.А. Применение методов оптимизации при выработке решений в обучении курсантов в образовательных организациях силовых структур. - Вестник Санкт-Петербургского университета МВД России. 2017. №2 (74). С. 165-173.
4. Большакова Л.В., Яковлева Н.А. Теория проверки статистических гипотез при математико-статистическом исследовании педагогических проблем. - Вестник Санкт-Петербургского университета МВД России. 2016. №4 (72). С. 149-158.

УДК 623.9

О ПЕРСПЕКТИВАХ ПРИМЕНЕНИЯ ПРОСТРАНСТВЕННО-ВРЕМЕННОГО КОДИРОВАНИЯ В РАДИОЛИНИЯХ ВМФ

Типикин Алексей Алексеевич[1], Пуха Геннадий Пантелеевич[2]
[1]ВУНЦ ВМФ «Военно-морская академия», Россия, Санкт-Петербург, Ушаковская наб 17/1
[2]Санкт-Петербургский государственный экономический университет
Россия, Санкт-Петербург, канала Грибоедова, 30/32
e-mails: alextip@mail.ru[1], pgp2003@list.tu[2]

Аннотация. В докладе обсуждается возможность применения способа ортогонального пространственно-временного кодирования для повышения достоверности радиолиний ВМФ декаметрового диапазона

Ключевые слова: *радиолиния; сообщение; электрический сигнал; достоверность; кодирование.*

ON THE PERSPECTIVES OF APPLICATION OF SPATIAL-TIME CODING IN THE RADIOLINIAS OF THE NAVY

Tipikin Alexey[1]. Pooh Gennady[2]
[1]VUNC Navy "Naval Academy", Russian Federation
St. Petersburg, Ushakovsky nab 17/1
[2]St. Petersburg State Economic University, Russian Federation
St. Petersburg, the Griboedov Canal, 30/32
e-mails: alextip@mail.ru[1], pgp2003@list.tu[2]

Abstract. The report discusses the possibility of applying the method of orthogonal space-time coding to increase the reliability of radio waves of the Naval Decameter range.

Keywords: *radio link; message; electrical signal; reliability; coding.*

Своевременная передача сообщений с учетом требований по достоверности и безопасности военной связи при всех воздействующих факторах зачастую рассматривается в качестве интегральной характеристики эффективности системы связи ВМФ [1]. Такой подход особенно характерен при исследовании систем связи тактического звена управления [2]. И действительно, процесс управления, оперативность которого во многом определяет успешность действий сил в этом звене, интересует, прежде всего, своевременность доставки, именно, достоверных сообщений с сокрытием при этом, факта его передачи и содержания [3].

В то же время, управление силами и оружием в современных боевых действиях требует передачи по системам связи сообщений все больших и больших объемов во все более жестких временных рамках, а значит - к ним предъявляются и все более высокие требования по пропускной способности [4, 5].

Обеспечение данных требований, в настоящее время идет, как известно, по направлению формирования в радиолиниях сложных многопозиционных сигнально-кодовых конструкций, повышающих спектральную эффективность радиолиний [6]. Однако при этом их энергетическая эффективность существенно снижается, так как для успешного своего функционирования им необходимо и лучшее соотношение сигнала и помехи, от которого, в конечном итоге, зависит достоверность принимаемых сообщений.

Следовательно, перед наукой и практикой стоит задача отыскания дополнительных возможностей по обеспечение достоверности связи вообще и передачи сообщений по радиолиниям ВМФ, в частности. Очевидно, что такую задачу следует решать, как на этапах проектирования и создания перспективных, так и совершенствования существующих систем связи ВМФ.

Обсуждение. Параллельным направлением обеспечение достоверности передачи сообщений по радиолиниям в целом, как известно, являются технические решения, направленные на обеспечение верности приема самого электрического сигнала и/или его элементов.

Одним из таких технических решений, например, стал способ ортогонального пространственно-временного кодирования, впервые предложенный С. Аламоути еще в 1998 г. [7].

Основные черты, характеризующие схему Аламоути, заключаются в следующем:

– для достижения максимального порядка разнесения не требуется обратной связи от приемника к передатчику, т.е. на передающей стороне информация о состоянии канала связи не используется;

– высокая простота реализации оптимального по критерию правдоподобия алгоритма приема;

– в схеме Аламоути может использоваться несколько приемных антенн N, но число передающих антенн при этом Мравно двум. Порядок разнесения в этом случае равен N*M за счет ортогональности передаваемых информационных сигналов.

Результаты моделирования показывают, что две передающие антенны и одна приемная дают такой же порядок разнесения, что и система сложения с максимальным отношением сигнал/шум (с оптимальным сложением) с одной передающей и двумя приемными антеннами [8].

Одним из важных преимуществ разнесения на передаче является то, что нет необходимости устанавливать несколько приемных антенн. Особенно это важно для систем с одним источником, передающим сообщения нескольким абонентам. Очевидна экономическая выгода относительно разнесения на приеме, которая состоит в установке дополнительного комплекта антенн только на передающей стороне. При этом на приемной стороне необходимо только устройство, реализующее алгоритм приема в соответствии со идеей метода. Примером такой системы может являться система передачи сообщений в направлении «Берег-корабль», где один передающий узел осуществляет передачу на все корабли в заданном районе.

Как следует из идеи метода, задача его практической реализации проще решается в диапазонах метровых (и выше) диапазонах волн. И именно поэтому, в настоящее время пространственно-временное кодирование, как часть MIMO-технологии, реализовано в нескольких беспроводных системах, включающих Wi-Fi, WiMAX и LTE, а также рекомендовано для перспективных стандартов, таких как LTE-AdvancediIMT-Advanced [9].

Однако исследования и соответствующих организационно-технических решений, связанных с применение данного способа повышения достоверности связи в подсистеме радиосвязи декаметрового диапазона пока, отсутствуют.

Очевидно, что основной проблемой здесь является реализация антенной системы, выполняющей разнесенную передачу, поэтому именно в этом направлении и потребуется провести дальнейшие исследования

СПИСОК ЛИТЕРАТУРЫ

1. Житов Ю.И. Комплексная методика оценки устойчивости системы связи ВМФ. — СПб. : 34 НИИ ВМФ, 2001. — 161 с.
2. Пуха Г.П. Анализ и синтез системы тактической связи группировок разнородных сил (учебно-методическое пособие для выполнения курсовых и дипломных работ). СПб., ВМА, 1995, 117 с.
3. Пуха Г.П. Методология формирования и реализации систем интеллектуальной поддержки принятия решений. – СПб., СМИО-Пресс, 2012. –337 с.
4. Арсланов Х.А., Абрамович А.В., Лихачев А.М. Концептуальные основы развития Объединенной автоматизированной цифровой системы связи Вооруженных сил Российской Федерации // Связь в Вооруженных силах Российской Федерации. — 2012. — С. 18-24.
5. Макаров Н.Е. Основные направления модернизации системы управления ВС РФ в современных условиях // Федеральный справочник. — 2010. — С. 217-144.
6. Верзун Н. А. Энергетическая эффективность помехоустойчивого кодирования в беспроводных сетях интернета вещей // Н. А. Верзун, А. М. Колбанёв, М. О. Колбанёв // Изв. вузов. Приборостроение. – 2017. – Т.60, № 2. – С.143–149.
7. Alamouti S.M. A simple transmit diversity technique for wireless communications // IEEE Journal on Selected Areas in Communications. — 1998. — Vol. 16, no. 8. — P. 1451-1458.
1. 8 Tarokh V., Jafarkhami H., Calderbank A.R. Space-time block codes from orthogonal designs // IEEE Transactions on Information Theory. — 1999. — Vol. 45, no. 5. — P. 1456-1467.
8. Brown T., De Carvalho E., Kyritsi P. Practical Guide to the MIMO Channel with MATLAB Examples. — New York : John Wiley and Sons, 2012. — 275 с.

УДК 332.1

СТРАТЕГИИ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РЕГИОНАЛЬНЫХ ЭКОНОМИЧЕСКИХ СИСТЕМАХ С УЧЕТОМ РАЗНЫХ ТИПОВ РЕАКЦИЙ НА ВЫЗОВЫ ВНЕШНЕЙ СРЕДЫ [2]

Титовец Алиса Юрьевна
Уральский государственный экономический университет
Россия, Екатеринбург, ул. 8 Марта, 62
e-mail: Alisa-2007-al@mail.ru

Аннотация. В статье рассматриваются перспективы и стратегические ориентиры развития информационных технологий в региональных экономических системах. Определена проблематика реализации государственной политики в области информационной безопасности и развития информационных технологий. Доказано, что барьером для развития информационных технологий в различных региональных экономических системах является разнокачественная территориальная реакция на инструменты воздействия. Описываются качественные характеристики понятий «временной реакционный буфер» и «реакция территорий (регионов или муниципалитетов)» и подчеркивается необходимость определения уровня и типа реакций на развитие и внедрение информационных технологий.

[2] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №17-32-00016 «Исследование реакций периферийных городских округов на изменение региональных экономических параметров в условиях реформирования местного самоуправления».

Ключевые слова: *информационные технологии; региональная экономическая система; реакция; временной реакционный буфер; безопасность; государственная политика.*

STRATEGIES OF INFORMATION TECHNOLOGIES DEVELOPMENT IN REGIONAL ECONOMIC SYSTEMS, BASED ON DIFFERENT TYPES OF REACTIONS TO THE CHALLENGES OF THE EXTERNAL ENVIRONMENT

Titovets Alisa
Ural State University of Economics
Russia, Yekaterinburg, 8 Marta str., 62
e-mail: Alisa-2007-al@mail.ru

Abstract. Prospects and strategic guidelines for information technologies development in regional economic systems have been discussed in the article. Problems of state policy implementing in the sphere of information security and information technologies development have been identified. It is proved that a barrier to the information technologies development in different regional economic systems is a territorial reaction to the tools of influence. Qualitative characteristics of such concepts like "timed reactionarybuffer" and “reaction of areas (regions or municipalities)" are described and need to identify the level and type of reactions for the development and implementation of information technology are emphasized.

Keywords: *information technologies; regional economical system; reaction; timed reactionary buffer; security; state policy.*

Каждая социально-экономическая трансформация общества осуществляется посредством новых технологий, которые существенно модифицируют производственные и экономические отношения. Экономика и общество современного мира находятся на стадии постиндустриального развития, который является этапом внедрения технических достижений второй половины XX века в экономические и общественные процессы. Интегрирование научных и технических достижений позволяет сформировать фундамент для перехода в новый технологический уклад.

Как отметил Президент РФ В.В. Путин «для выхода на новый уровень развития экономики, социальных отраслей нам нужны собственные передовые разработки и научные решения. Необходимо сосредоточиться на направлениях, где накапливается мощный технологический потенциал будущего, а это цифровые, другие, так называемые сквозные технологии, которые сегодня определяют облик всех сфер жизни» [15]. Прежде всего, это информационные технологии и компьютеризированные системы, высокие производственные технологии, являющиеся результатом новых открытий и изобретений.

Как отмечают В. Новиков и Е. Ткачёва «новые трансформации экономического пространства и информационные возможности вызывают к жизни новые информационные мотивы и потребности, развитие и удовлетворение которых приводит к модификации и в экономике, и в повседневной жизни» [14].

Поэтому устойчивое социально-экономическое развитие – это поиск и выбор среди имеющихся альтернатив такого способа развития, при котором достижение определённых целей в настоящем времени будет способствовать их достижению в будущем [11].

На территории РФ функционирует и реализуется несколько стратегических документов в области развития информационных технологий и информационного общества:

1) ФЗ О безопасности критической информационной инфраструктуры Российской Федерации

2) Доктрина информационной безопасности Российской Федерации

3) Стратегия развития информационного общества в Российской федерации на 2017-2030 годы

4) Стратегия Развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года

5) Программа "Цифровая экономика Российской Федерации"

6) План мероприятий ("дорожная карта") "Развитие отрасли информационных технологий"

7) Концепция региональной информатизации.

В рамках данных документов определено, что информационные технологии являются инструментом формирования информационного общества, цифровой экономики и эффективной системы взаимодействия всех уровней власти между собой, бизнесом и населением. Внедрение, развитие и создание информационных технологий позволит стране в целом сформировать конкурентоспособную экономику на мировом уровне, а самое главное, последние принятые документы нацелены на повышение уровня безопасности страны и населения от внешних угроз. Информационные технологии стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка, а повсеместное внедрение иностранных информационных технологий усложняет решение задачи по обеспечению защиты интересов граждан и государства в информационной
сфере [3].

Анализ документов стратегического планирования, позволяет сделать вывод, что новый вектор развития информационных технологий в контексте территориального развития снова выстраивается по прошлому сценарию. С акцентом только на общих вопросах развития данной области, без учета специфики регионов или муниципалитетов, без понимания что одни и те же инструменты не могут сработать на разных территориях одинаково и без учета прошлых ошибок.

По мнению Гусакова М.А. «... в нашей стране в последние 10 и более лет реализовывался инерционный сценарий развития науки и технологии, не произошло принципиальных изменений в отношении динамики технологического и инновационного развития» [10]. И, по его мнению, единственной возможностью запустить нормальный процесс развития науки и технологий это « ... вовлечение максимального числа регионов ...» [10].

Для вовлечения максимального количества регионов и муниципалитетов в данный процесс, необходимо учитывать уровень экономико-технического развития территории, который определяет возможность субъекта или муниципалитета реализовать стратегические информационные мероприятия. Поэтому при формировании вектора развития информационных технологий в территориальном аспекте необходимо, на наш взгляд, в первую очередь оценить степень реагирования региональной или муниципальной системы на новые изменения и условия. Изучение данного вопроса, позволяет сделать вывод, что в современном мире для эффективного развития территориальных экономических и общественных систем необходимо учитывать реакцию данной системы, как живого организма и сложной системы, на угрозы и факторы развития.

Галазова С.С. отмечает что «исследования по соответствующей тематике находятся фактически на начальной стадии. Поэтому сегодня имеются все основания оценивать ситуацию как этап формирования методологической и теоретической базы изучения реакции региональных социально-экономических систем на изменения национальных макроэкономических параметров и институциональных условий. Тем не менее, уже сложилась фундаментальная основа для реализации выбранного направления исследования как особого фактора становления региональной экономики и того, что этим обусловлено – процесса формирования региональной экономической политики» [9].

При этом данное направление исследования имеет огромное значение для России в целом и для конкретных регионов (муниципалитетов) - субъектов федерации, высокий уровень нестабильного и дифференцированного развития регионов страны приводит к неэффективному функционированию всей системы, которая по кругу задевает все регионы (не стабильность "проблемных регионов" - не стабильность страны - не стабильность "сильных" регионов).

Понимание сложности реакции и ее неравномерности по всей территории страны, приводит необходимости выделения такого явления как "временной реакционный буфер". Отталкиваясь от того, что регионы не просто по-разному реагируют на внешние факторы, но и в разное время, то есть наблюдается в действие теория "центр-периферия" и возникает ситуация отложенной во времени региональной реакции.

Это приводит к тому, что некоторые территории достаточно быстро показывают результат по внедрению информационных технологий и начинают получать информационные выгоды, а некоторые территории не в состоянии внедрить информационные технологии, так например, ОМСУ сельских территорий не могут создать свой сайт не потому что у них нет финансовых средств или специалистов, а потому что скорость Интернета на их территориях настолько низкая, что им просто не имеет смысла его делать, его никто не сможет загрузить и использовать.

То есть экономически сильные регионы, смогут эффективнее и быстрее перетягивать положительные факторы развития, так Зубаревич Н.В. отмечает, что «…процессы глобализации ранее всего проявились в крупнейших городских агломерациях...» [12]. Данный феномен приводит к неравномерности развития территорий страны и под влиянием "положительных" факторов остается и даже усиливается.

На этот аспект обращают внимание Глушков А.И. и Цало И.М. отмечая, что «в городах федерального значения экономическая реакция на значительные изменения тенденций на мировых рынках происходит крайне быстро, тогда как в региональных городах экономическая реакция отложена во времени». Это связано с тем, что данные территории сильнее вовлечены и зависимы от мировых рынков.

Поэтому временной реакционный буфер для каждого региона будет свой, в зависимости от уровня развития территории, соответственно и деятельность органов власти на данных территориях должна быть разной. Соответственно, существует необходимость классификации видов реакций региональных экономических систем и типологизации регионов РФ с точки зрения реакций.

В работе Лымарева М.И. отмечено, что необходима особая «рефлексивная» типология российских регионов по степени, факторам и результатам их реакции на динамику макроэкономических параметров и разработка рекомендаций по выбору наиболее эффективных инструментов воздействия федеральных экономических индикаторов на развитие экономики того типа [13].

Формирование стратегических документов и федеральной политики с учетом "реакционности" территории на инструменты воздействия позволит эффективно и рационально использовать

имеющие ресурсы необходимые для развития. Соответственно необходимо разработать классификацию реакций регионов (муниципалитетов) на внешние и внутренние изменения с учетом специфики территорий.

Можно отметить, что существует необходимость учета и повышения устойчивости экономики к воздействиям, в том числе и на региональном уровне, проскальзывает в стратегическом документе "Стратегия экономической безопасности Российской Федерации на период до 2030 года". В рамках данного документа четко выделяется задача по формированию «сбалансированного пространственного и регионального развития Российской Федерации, укрепления единства ее экономического пространства» от внешних и внутренних вызовов и угроз [2].

Но даже с учетом данного документа, можно четко определить, что перед всеми регионами и муниципалитетами ставятся одни те же цели и задачи по развитию информационной экономики, информационного общества и информационных технологий, без учета региональной или муниципальной специфики.

Такими основными задачами являются:

- повышение качества жизни;
- увеличение вклада отрасли информационных технологий в ВРП и ВВП;
- обеспечение конкурентоспособности экономики и технологического развития;
- создание и развитие информационной структуры;
- повышение эффективности государственного и муниципального управления;
- создание и развитие ИТ- кластеров;
- повышение уровня обеспеченности кадрами ИТ отрасли.

Из выше изложенных задач, можно сделать вывод, что успеха добьются в развитии информационных технологий, только те регионы и муниципалитеты, которые имеют базу и экономические возможности для этого. В принципе сейчас это и происходит в стране, так как позитивными результатами в данной области могут похвастаться только г. Москва, г. Санкт - Петербург и Республика Татарстан, остальные регионы не достигли и не сформировали нужный информационный уровень развития, а соответственно и уровень безопасности. Но здесь все намного сложнее, так одно не работающее звено в цепи информационной безопасности приводит к краху всей цепи. При этом, если проблематика регионального уровня хотя бы поднимается, то муниципальный уровень остается без внимания.

Заключение. Один из самых сложных аспектов функционирования регионов в современных реалиях – это реагирование на постоянные изменения во внешней и внутренней среде. Так как XXI век не только сформировал уникальные возможности для внедрений и развития информационных технологий, но усилил проблематику безопасности. Поэтому с учетом специфики территориального уровня развития России, при формировании стратегических документов информационного развития необходимо учитывать разные типы реакции территорий. Все это обуславливает сложность реализации принятых решений на региональном и муниципальном уровнях и невозможность реализации их традиционными методами и способами и приводит к необходимости определения типов, уровней и масштаба реакции регионов или муниципалитетов, формирования классификации реакций.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 5.12.2016 г. № 646.
2. Стратегия экономической безопасности Российской Федерации на период до 2030 года: Указ Президента РФ от 13.05.2017 N 208.
3. Стратегия развития информационного общества в Российской федерации на 2017-2030 годы: Указом Президента РФ от 9.05.2017 г. № 203.
4. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 N 187-ФЗ.
5. Стратегия Развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года: Распоряжение Правительства РФ от 01.11.2013 N 2036-р.
6. План мероприятий ("дорожная карта") "Развитие отрасли информационных технологий": Распоряжение Правительства РФ от 30.12.2013 N 2602-р.
7. Концепция региональной информатизации: Распоряжение Правительства РФ от 29.12.2014 N 2769-р.
8. Программа "Цифровая экономика Российской Федерации": Распоряжение Правительства РФ от 28.07.2017 N1632-р.
9. Галазова С.С. Пространственный аспект современной экономической теории // Terra Economicus. 2014. Т. 12. № 2-2. С. 6-10.
10. Гусаков М.А. Выявление направлений и путей трансформации научно-инновационного пространства регионов разного типа // Экономические и социальные перемены: факты, тенденции, прогноз 2014. 3 (33). с. 151-168.
11. Ефимова Е.Г. Развитие региональной социоэкономической системы как новая возможность экономического роста // Материалы II международной научно-практической конференции «Актуальные вопросы экономических наук» - Астана: Мастер По ЖШС, 2017. – 617 с.
12. Зубаревич Н.В. Крупнейшие города России как «агенты» глобализации // Россия и современный мир. 2002. № 4 (37). С. 97-101
13. Лымарев М.И. Макроэкономические приоритеты региональной динамики // Экономический вестник Ростовского государственного университета, 2008 г.Том 6 (№2). Часть 2
14. Новиков В.С., Ткачева Е.Н. Виртуальное экономическое пространство в глобализирующейся системе региональной экономики // Региональная экономика: теория и практика. 2012 г. № 7. С. 53–58.
15. Послание Президента Федеральному Собранию 01.12.2016 года // http://kremlin.ru

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА ИТ-СПЕЦИАЛИСТОВ

УДК 004.056.53

РЕАЛИЗАЦИЯ КОМПЕТЕНТНОСТНОГО ПОДХОДА ПРИ ФОРМИРОВАНИИ ПООП НОВОГО ПОКОЛЕНИЯ НА ПРИМЕРЕ ЛАБОРАТОРНОГО ПРАКТИКУМА «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

Барабаш Павел Александрович, Панасенко Михаил Александрович
Смольный институт Российской академии образования
Россия, Санкт-Петербург, Полюстровский пр., 59
e-mails: barabash_p@yahoo.com, panasenko16.01.93@mail.ru

Аннотация. Вдокладе обсуждаютсявопросы реализации компетентностного подхода при формировании примерной образовательной программы(ПООП) подготовки бакалавра в рамках ФГОС нового поколения на примере лабораторного практикума «Безопасность информационных систем». Рассматриваются подходы к выбору структурыи содержания примерного лабораторногопрактикума с учетом формируемых профессиональных компетенций и сопряженных профессиональных стандартов.

Ключевые слова: *информационные системы и технологии; безопасность информационных систем; профессиональные компетенции; сервер безопасности; система защиты информации; учетные записи; профессиональные стандарты.*

REALIZATION OF COMPETENCE-BASED APPROACH WHEN FORMING POOP OF NEW GENERATION ON THE EXAMPLE OF THE LABORATORY PRACTICAL WORK «SAFETY OF INFORMATION SYSTEMS»

Barabash Pavel, Panasenko Mikhail
SmolnyInstitute of the RussianAcademy of Education
Russia, St. Petersburg, Polyustrovsky pr., 59
e-mails: barabash_p@yahoo.com, panasenko16.01.93@mail.ru

Abstract. In the report issues of realization of competence-based approach when forming the approximate educational program of training of the bachelor within FGOS of new generation on the example of a laboratory practical work "Safety of information systems" are discussed. Approaches to the choice of structure and the maintenance of an approximate laboratory practical work taking into account the formed professional competences and the interfaced professional standards are considered.

Keywords: *information systems and technologies; safety of information systems; professional competences; safety server; system of information security; accounts; professional standards.*

Введение. В соответствии с проектом примерной образовательной программы подготовки бакалавра по в рамках ФГОС нового поколенияпо направлению 09.03.02 Информационные системы и технологии учебная дисциплина «Безопасность информационных систем» относится к вариативной части учебного плана и нацелена на формирование следующих компетенций:

– понимание сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности (ОПК-4);

– владение основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий (ОК-12);

– знание своих прав и обязанностей как гражданина своей страны, способность использовать действующее законодательство и другие правовые документы в своей деятельности, демонстрировать готовность и стремление к совершенствованию и развитию общества на принципах гуманизма, свободы и демократии (ОК-9).

В общей трудоемкости учебной дисциплины (более 100 часов), соотношение лекционных и лабораторных работ 2:3. При этом лекционный курс состоит из 3 модулей и включает 12 тем, позволяющих сформировать у студентов представление о механизмах обеспечения безопасности информационных систем [2, 3]. Для закрепления навыков практической работы со специальными программными средствами защиты информации разработан примерный комплекс лабораторных работ, структурная схема которого представлена на рис. 1.

В компьютерном классе устанавливается ПО виртуализации - Microsoft Virtual PC 2007 SP1, позволяющее запустить две виртуальные машины. На первой виртуальной машине устанавливается Windows Server 2003 и «Сервер безопасности» Dallas Lock, которые, в частности, выполняют роли Контроллера домена, Файлового сервера, DNS – сервера и позволяют выполнить настройку правил «Сервера безопасности» Dallas Lock8.0, предоставляющего следующие возможности:

- централизованное управление пользователями и группами пользователей на клиентах;
- централизованное управление политиками безопасности клиентов;
- централизованный сбор журналов с клиентов;
- управление доступом к ресурсам файловой системы и к устройствам на клиентах;
- просмотр состояния отдельных клиентов;
- объединение клиентов в группы.

Некоторые параметры безопасности могут быть настроены сразу для всего Домена безопасности, некоторые – для групп клиентов, некоторые – для отдельных клиентов.

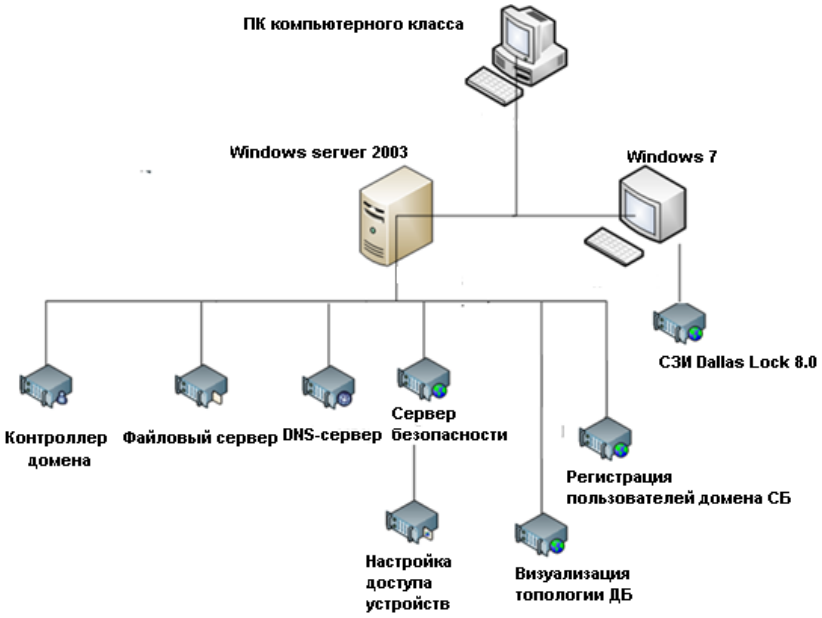


Рис.1 Структурная схема лабораторного комплекса

На вторую виртуальную машину устанавливается ОС Windows 7 и средство защиты информации (СЗИ) Dallas Lock 8.0, предназначенное для изучения студентами возможностей этого программного продукта. Выбор этих программных продуктов диктуется техническими параметрами ПК в компьютерном классе, а также особенностями Dallas Lock 8.0, приведенными в таблице 1.

Таблица 1

Характеристики Dallas Lock 8.0-С

Наименование параметра	Значение параметра
Тип СЗИ	Программно-аппаратный комплекс
Сертификат соответствия ФСТЭК России	№ 2945 от 16.08.2013 г. действителен до 16.08.2019 г.
Класс защищенности СВТ	3
Класс защищенности МЭ	3
Класс защиты СОВ	4
Класс защиты СКН	2
Уровень контроля отсутствия НДВ	2
Авторизация до загрузки ОС	Да
Мандатный принцип разграничения доступа	Да
Единый реестр российских программ для ЭВМ и БД	Приказ Минкомсвязи России № 151 от 08.04.2016 г.

Рассмотрим основные цели и задачи, решаемые каждой из 10 лабораторных работ.

– ознакомление студентов с процессами загрузки виртуальной машины и установки на ней Windows Server 2003, приобретение навыков установки виртуальной машины с помощью Мастера установки, настройки параметров домена, установки DNS сервера и др.;

– знакомствос общими принципами работы сервера безопасности и приобретение навыковпо его установке. (Сервер безопасности (СБ) реализован в виде службы, которая автоматически запускается при подключении к ПК лицензионного ключа СБ; управление СБ осуществляется программой «Консоль сервера безопасности»; для установки СБ студентам необходимо запустить программу «Dallas Lock 8.0 Сервер безопасности»);

– изучение вопросов администрирования сервера безопасности (СБ), знакомство с работой с консолью СБ (КСБ), приобретение навыков по администрированию СБ, изучение инструментов КСБ, работа в консоли СБ, работе с клиентами Windows из консоли управления. (С помощью КСБ можно настроить параметры безопасности для следующих объектов: Домена безопасности(ДБ), определив настройки при выборе объекта, обозначающего СБ в дереве объектов КСБ; для группы клиентов, определив настройки при выборе объекта, обозначающего группу в дереве объектов КСБ; для индивидуального клиента, выбрав его объект в дереве КСБ. Для дальнейшей работы студентам необходимо с помощью Мастера установить новую виртуальную машину Windows и установить на ней ОС Windows 7);

– приобретение навыков устанавкисистемы защиты информации (СЗИ) Dallas Lock 8.0 на виртуальную машину;

– знакомство с подсистемой управления доступом Dallas Lock 8.0 и полномочиями на управление этой системой, приобретение навыков регистрирации иудалению пользователей, просмотра и редактирования учетных записейс получением соответствующих полномочий администратора;

– знакомство с технологией и этапами отладки управления доступом и полномочиями на управление учетными записями; приобретение навыков создания учетных записей, создания и и удаления группы пользователей, регистрации доменных пользователей, регистрациидоменных учетных записей по маскеи др.;

– знакомство с возможностями тонких настроек учетных записей в СЗИ, связанных, в частности, с определением числа разрешенных сеансов для данной учетной записи, сменой пароля для авторизации средствами ОС, сменой пароля с помощью оболочки администратора, работой с сессиями-исключениями, работой с заблокированными пользователями, проверкой количества одновременных интерактивных и сетевых сессий (входов);

знакомство с вариантами тонкой настройки учетных записей для контроля доступа и устройств, в частности, с настройкой полномочий на управление контролем устройств, разграничением доступа к устройствам, разграничением доступа к устройствам и мандатного доступа. (В разных версиях ОС Windows в диспетчере устройств одно и то же физическое устройство может идентифицироваться по-разному; это следует учитывать при определении прав доступа к устройству/классу устройств, особенно при централизованной настройке средствами Сервера безопасности и при назначении мандатных уровней для доступа к устройствам. Установка мандатного доступа на устройство происходит путем определения уровней конфиденциальности в дескрипторе объекта, для работы под которыми устройство должно быть доступно. На рис. 2. показано окно настройки мандатного доступа);

знакомство с вариантами тонкой настройки учетных записей для настройки Домена безопасности и работы с ним в среде СБ, приобретение навыков ввода клиента в Домен безопасности, ввода защищенного компьютера в ДБ, вывода клиента из ДБ, настройки ДБ, настройки сервера лицензий для СБ, визуализации топологии ДБ. (При этом в рабочей области визуализации сети отображается многоуровневая архитектура ДБ: Сервер безопасности, группы клиентов Сервера безопасности, клиенты. С помощью панели действий можно добавлять и редактировать надписи в топологии, возвращать измененную топологию в исходное состояние).

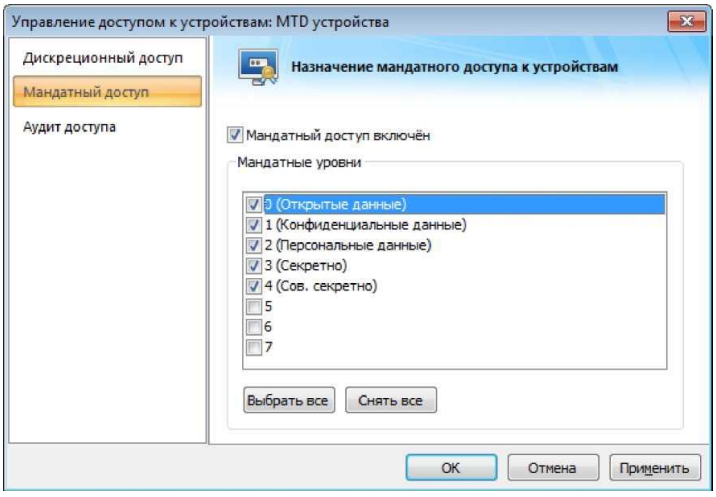


Рис. 2. Настройка мандатного доступа

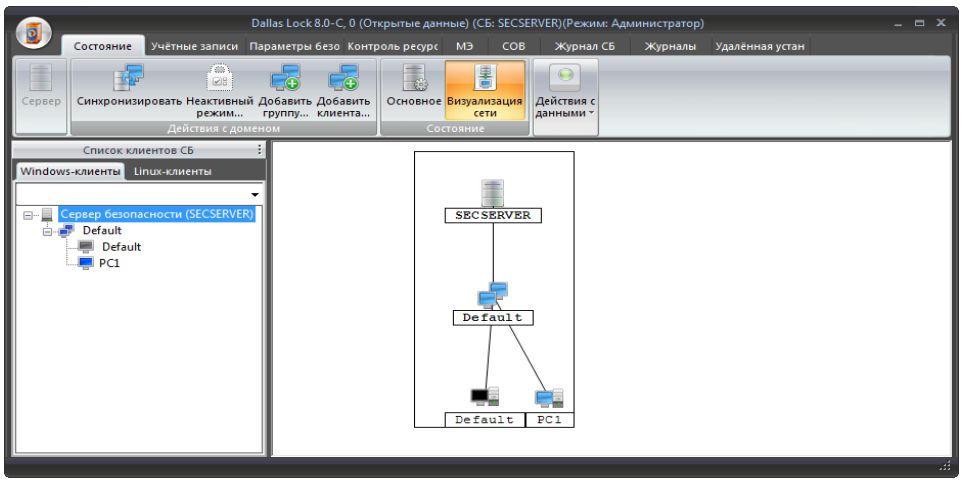


Рис. 3. Визуализация топологии Домена безопасности

После выполнения каждой лабораторной работы студенты создают отчет, представляющий собой текстовый файл, оформленный в соответствии с определенными требованиями, содержащий скриншоты (снимки экрана компьютера) операций с описанием процедур выполнения. Отчет размещается в личном кабинете электронной образовательной среды института. Таким образом, формируется часть портфолио студента, в соответствии с требованиями ФГОС ВО [1].

Заключение. Рассмотренная структура и содержание разработанного лабораторногопрактикума «Безопасность информационных систем» может быть использована для обсуждения возможных подходов к реализации компетентностного подхода при формированиипримерной образовательной программы подготовки бакалавра в рамках ФГОС нового поколения с учетом приобретаемых профессиональных компетенций и сопряженных профессиональных стандартов.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный государственный образовательный стандарт высшего образования. Уровень высшего образования Бакалавриат. Направление подготовки 09.03.02 Информационные системы и технологии. (Министерство образования и науки РФ, приказы № 219 от 12.03.2015 г., № 999 от 09.09.2015 г.).
2. Барабаш П.А., Воробьев С.П., Курносов В.И., Советов Б.Я. Инфокоммуникационные технологии в Глобальной информационной инфраструктуре – Санкт-Петербург. : Наука, 2008, 552 с.
3. Безопасность персональных данных. Учебное пособие /П.А. Барабаш. – СПб. : Политехника, 2012. – 167 с.

УДК 378

ПРОФЕССИОНАЛЬНЫЙИ ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТЫ КАК ОСНОВА ВЗАИМОДЕЙСТВИЯ ОБРАЗОВАНИЯ, НАУКИ И ОТРАСЛЕВЫХРАБОТАДАТЕЛЕЙ В КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННОЙ ПОДГОТОВКЕ БУДУЩИХ КАДРОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕХНИЧЕСКОМ ВУЗЕ

Жигадло Анна Валентиновна[1], Одинокая Мария Александровна[2]
[1]ООО «ГАЗПРОМНЕФТЬ-ЦЕНТР»
Россия, Санкт-Петербург
[2]Санкт-Петербургский политехнический университет Петра Великого
Россия, Санкт-Петербург, ул. Политехническая, 29
e-mails: Zhigadlo.Anna@gmail.com,World.Maria@hotmail.com

Аннотация. В докладе обсуждается роль профессиональных и образовательных стандартов в компетентностно-ориентированной подготовке студентов технического вуза.

Ключевые слова: *компетентностно-ориентированная подготовка; профессиональные стандарты; образовательные стандарты; трудовые функции; технический вуз.*

PROFESSIONAL AND EDUCATIONAL STANDARDS AS THE BASIS OF THE INTERACTION AMONG EDUCATION, SCIENCE AND INDUSTRY EMPLOYERS IN COMPETENCE-ORIENTED TRAINING OF SPECIALISTS IN THE SPHERE OF INFORMATION SECURITY IN TECHNICAL UNIVERSITY

Zhigadlo Anna[1], Odinokaya Mary[2]
[1]GAZPROM NEFT - CENTER Ltd.
Russia, St. Petersburg
[2]Peter the Great St. Petersburg Polytechnic University
Russia, St. Petersburg, Politehnicheskaya str., 29
e-mails: Zhigadlo.Anna@gmail.com,World.Maria@hotmail.com

Abstract. The report isfocused on the role of professional and educational standards in the competence oriented preparation of students of technical university.

Keywords: *competence oriented training; professional standards; educational standards; labor functions; technical university*.

Качество высшего образования и одного из аспектов образования - образовательного процесса является приоритетным направлением российского педагогического общества. Под качеством образовательного процесса понимается совокупность его существенных характеристик, соответствующих заданной стандартами государственной норме и способных удовлетворить ожидания студентов, бизнес-сообществ, государственных структур. Для обеспечения гибкой системы профильного обучения в техническом вузе особую роль приобретают информационно-коммуникационные технологии, предусматривающие синергию образовательного потенциала образовательных учреждений, включая учреждения начального, среднего, высшего профессионального и дополнительного образования.

На современном этапе наличие профессиональных стандартов, в частности, в отрасли информационной безопасности, способствует обновлению процесса профессионального обучения в техническом вузе с учетом изменяющихся требований работодателей, оценки качества образовательного продукта в соответствии с потребностями российского рынка труда и требованиям бизнес-сообществ.

Под профессиональным стандартом понимается нормативный документ, определяющий в области профессиональной деятельности нормативные требования к квалификации рабочей силы со стороны работодателя, в частности наборы профессиональных компетенций, и коррелирующий с образовательными стандартами.

Особая роль при реализации компетентностного подхода отводится использованию в образовательном процессе активных и интерактивных форм проведения учебных занятий в сочетании с внеаудиторной работой. Именно при интерактивной форме проведения любых занятий в большей степени формируются личностные аспекты профессиональных компетенций, которые представляются нам весьма важными [2].

Система профессиональных стандартов является основой для разработки образовательных стандартов, обеспечивающих сопряжение требований российского рынка труда и сферы образования [1]. Задание требований к уровню подготовки выпускников в профессиональной деятельности должно определять содержание образовательных стандартов. Оценка качества профессиональной подготовки будущих кадров в сфере информационных технологий в современном техническом вузе зависит от качества разработки профессиональных стандартов, учитывающих современные требования к профессиям и квалификациям выпускников профессиональных образовательных организаций. Необходимо активизировать совместную деятельность рынка труда и сферы образования в России по разработке и внедрению устойчивого и эффективного механизма взаимодействия и достижению профессионального стандарта различными путями.

СПИСОК ЛИТЕРАТУРЫ

1. Горшкова О.В., Фалько Л.Ю. Профессиональные стандарты: практикаразработки и внедрения в России // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса, №5, 2012, С. 93-103.
2. Одинокая М.А. Современные технологии интерактивного обучения в многопрофильном вузе / М.А. Одинокая, Н.В. Попова. – СПб.: Изд-во Политех. Ун-та, 2016. – 258 с.

УДК 378

ОСОБЕННОСТИ ПРОФЕССИОНАЛЬНОЙ И ОБРАЗОВАТЕЛЬНОЙ СТАНДАРТИЗАЦИИ В СФЕРЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СОВРЕМЕННОЙ ВЫСШЕЙ ШКОЛЕ

Жигадло Надежда Владимировна
Россия, Санкт-Петербург, Гимназия № 652
e-mail: World.Maria@hotmail.com

Аннотация. В докладе рассматривается роль профессиональных и образовательных стандартов в компетентностно-ориентированной подготовке IT-специалистов по специальности информационная безопасность.

Ключевые слова: *компетентностно-ориентированная подготовка; IT-специалист; профессиональные стандарты; образовательные стандарты; трудовые функции; компетенции*.

THE ROLE OF PROFESSIONALAND EDUCATIONAL STANDARDSINTHESPHERE OFINFORMATIONTECHNOLOGIES

Zhigadlo Nadezhda
Russia, St. Petersburg, Gymnasium № 652
e-mail: World.Maria@hotmail.com

Abstract. Thearticleis focused on theroleofprofessional and educational standards in the competence oriented preparation of IT-specialists in an information security.

Keywords: *competence oriented training; IT-specialist; professional standards; educational standards; laborfunctions; competences.*

В современной высшей школе, при подготовке выпускников технических направлений профессиональные IT-стандарты выступают в роли эталона содержания вузовской подготовки, и также могут быть ориентиром разработки подходов к оценке качества профессиональной подготовки будущих профессиональных кадров в вузе.

Под профессиональным стандартом понимается документ, раскрывающий с позиций сферы труда (объединений работодателей) содержание трудовых функций работника конкретного вида экономической деятельности (области профессиональной деятельности) и необходимых для их выполнения компетенций по различным квалификационным уровням, а также ряд других параметров, характеризующих специфику труда. Под образовательным стандартом понимается совокупность обязательных требований к высшему образованию по специальностям и направлениям подготовки образовательными организациями высшего образования, определенным перечнем, утверждаемым указом Президента Российской Федерации [1]. Профессиональные и образовательные стандарты являются составной частью национальной системы квалификаций, в которую также входят национальная рамка квалификаций (уровни квалификаций), отраслевые рамки квалификаций, система независимой оценки результатов образования и сертификации.

Именно через механизм профессиональных стандартов работодатели сообщают сфере образования о содержании профессиональной деятельности в рамках определенного вида экономической деятельности и требованиях к квалификации работников, образовательные учреждения с учетом этих требований осуществляют подготовку специалистов, соответствующих актуальным и перспективным потребностям рынка труда. В области ИТ-технологий профессиональный стандарт способствует контролю стандартов качества IT-деятельности, определять уровень профессионализма работников. Задача высшего образования является более широкой, чем подготовка человека к работе по определённой профессии. В нее входит его саморазвитие, личностное и профессиональное, в том числе и способность переучиваться и работать по новым профессиям, в том числе и по тем, которые в настоящий момент ещё не существуют.

Очевидно, что консолидация образовательной и профессиональных сфер становятся необходимой реальностью. Необходима дальнейшая популяризация идеи профессиональных и образовательных стандартов как в сфере образования, так и в бизнес-сфере. Для высшего образования профессиональные стандарты, в частности IT-стандарты по информационной безопасности необходимы для формирования образовательных стандартов, основных образовательных программ, учебных планов, а также для разработок образовательных ресурсов в формате e-learning как для студентов, так и для преподавателей.

СПИСОК ЛИТЕРАТУРЫ

1. Махотин Д.А. Профессиональные и образовательные стандарты: соотношение требований к современному педагогу // Вестник МРАТ, №2-3 (5-6), 2012, С. 89-100.

УДК 364

ДИСТАНЦИОННОЕ ОБУЧЕНИЕ КАК ОПЕРАЦИОННО-ДИДАКТИЧЕСКАЯ ФОРМА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПЕДАГОГИЧЕСКИХ КАДРОВ В СИСТЕМЕ НЕПРЕРЫВНОГО ОБРАЗОВАНИЯ ВЗРОСЛЫХ

Каткова Ирина Васильевна, Цесаренко Ольга Петровна
Смольный университет Российской академии образования
Россия, Санкт-Петербург, Полюстровский пр.,59
e-mail: avtofakultet@mail.ru

Аннотация. В статье рассмотренаоперационно-дидактическая форма повышения квалификации педагогических кадров в системе непрерывного образования взрослых.

Ключевые слова: *непрерывное образование; операционно-дидактическая форма; дистанционное образование; образовательные технологии.*

DISTANCE EDUCATION AS OPERATIONALLY DIDACTIC FORM OF PROFESSIONAL DEVELOPMENT OF PEDAGOGICAL STAFF IN CONTINUING EDUCATION ADULTS

Katkova Irina, Cecarenko Olga
Smolny Institute of the Russian Academy of Education
Russia, St. Petersburg, Polyustrovskiy pr., 59
e-mail: avtofakultet@mail.ru

Abstract. The article considers operational and didactic form of professional development of pedagogical staff in continuing education of adults.

Keywords: *continuous education; operational-didactic form; distance education; educational technology.*

Введение. Потребность учиться в течение всей жизни вызвана прежде всего быстрыми изменениями в социально-экономическом развитии, техническом оснащении производства, быстрым старением знаний. Интенсивный рост потока информации через каждые 5-10 лет обусловливает необходимость обновления знаний, чтобы соответствовать актуальным требованиям жизни. Проведенные за рубежом исследования показывают, что даже лучшие высшие учебные заведения не считают, что они выпускают специалистов, образование которых уже завершено. Таким образом, Образовательная система в информационном обществе должна стать системой опережающей. Переход от консервативной образовательной системы к опережающей должен базироваться на опережающем формировании информационного пространства Российского образования.

Отметим, что в связи с переходом индустриальных и постиндустриальных стран к информационному обществу образование, и прежде образование взрослых, становится объективной, реальной потребностью большинства, носит всеобъемлющий характер. Для нашего исследования важное значение имеют научные труды, в которых изложены идеи непрерывности образования в соответствии с потребностями человека (С. Батышев, А. Беляева, Н. Кузьмина, В. Леднев, Н. Ничкало, В. Онушкин и др.).

Образование взрослых не может рассматриваться обособленно, поскольку оно является общей составляющей системы непрерывного образования и осуществляется в течение всей жизни, включая все области знаний, используя максимальные возможности для развития личности, получения новой или повышения существующей квалификации, участия в социально-экономической жизни общества. Процессы образования, в которых принимают участие дети, молодежь, взрослые, рассматриваются как единое целое.

Человек учится постоянно, без относительно длинных перерывов или в образовательных учреждениях, или средствами самообразования. Он включен в образовательный процесс на всех стадиях его развития с учетом наследственности при переходе с одной ступени к другой [1]. Одновременно можно выделить некоторые принципы, на которых базируется дистанционное образование взрослых: учет личностных качеств (возраст, семейное положение, профессиональный и социальный статус, физическое и психологическое состояние здоровья и другие факторы); использования практического и жизненного опыта, ведь благодаря ему, взрослые являются носителями новых знаний, умений, культуры, это способствует тому, что одновременно они учатся сами и обучают других;признание того, что в определенной ситуации или на определенном периоде образование взрослых может играть компенсирующую роль, оно не предназначено для замены соответствующего образования молодежи, что в свою очередь является успешной предпосылкой образования взрослых.

Независимо от форм организации дистанционное обучение – это особая, завершенная форма, имеющая элементы наглядного, наглядно-заочного, заочного и вечернего обучения на основе информационных технологий и систем мультимедиа. Комплекс образовательных услуг, предоставляемых с помощью специализированной информационно-образовательной среды на любом расстоянии от образовательных учреждений, определяет дистанционное образование как одну из форм непрерывного образования, образования «на протяжении жизни».

Характерными чертами дистанционного образования является гибкость, модульность, экономичность, технологичность, социальное равенство, интернациональность, новая роль преподавателя, качество и др.

Роль преподавателя в дистанционном образовании расширяет и обновляет роль преподавателя, делает его наставником-консультантом, который должен координировать познавательный процесс, постоянно совершенствовать те курсы, которые он преподает, повышать творческую активность и квалификацию в соответствии с нововведениями и инновациями. На преподавателя возлагается новая роль. Он координирует процесс обучения на основе видоизмененного курса, проводит консультации при составлении индивидуального учебного плана, руководит учебными проектами, направляет обучение групп взаимоподдержки, помогает слушателям, в их профессиональном самоопределении. На основе анализа отечественной и зарубежной теории и практики организации повышения квалификации педагогических кадров показано, что этим требованиям может удовлетворять операционно-дидактическая система, выстроенная как форма, в которой должны быть воплощены особенные принципы непрерывного образования.

Непрерывное образование – процесс и принцип формирования личности, предусматривающий создание таких систем образования, которые открыты для людей любого возраста и поколения и сопровождают человека в течение всей его жизни, способствуют постоянному его развитию, вовлекают в непрерывный процесс овладения знаниями, умениями, навыками и способами

поведения (общения). Операционно-дидактическая форма - упорядоченный набор целей, содержания, форм, методов и средств обучения.

Основу процесса обучения как дидактической системы составляет учебная деятельность. Учебная деятельность выполняется человеком на протяжении всей его жизни. Дистанционное образование - это организационная форма, при которой коммуникация между обучающимся и обучающим осуществляется по преимуществу опосредованно на расстоянии на основе использования самых разнообразных средств.

Образовательные технологии - это внедрение основных направлений педагогической стратегии, которая достигается программой и стандартом образования целей по конкретному учебному предмету. В государственной стратегии развития России важнейшими целями модернизации образования признаются: развитие интеллектуального потенциала личности, аналитических способностей, критического мышления, которое достигается в системе непрерывного образования. Развитие умений самоанализа и осознания собственных возможностей, постоянное пробуждение творческих способностей, инициативы, развитие коммуникабельности и выработка способности оперативно и эффективно решать возникающие проблемы, позволяет опережающему образованию, включить в себя операционно-дидактические формы. Такое образование является важнейшим методологическим принципом дальнейшего развития профессионального образования, требующим пересмотра сложившихся стереотипов.

Основная цель профессионального образования взрослого человека – профессиональное развитие личности.

Опережающее обучение – осуществляется на основе прогнозирования научно-технического развития общества и условий труда, ориентации полученных знаний и умений и одновременно развитие потенциала компетентности специалиста.

Основные принципы опережающего образования – развитие адаптивности, мобильности, конструктивности субъективной ориентации, личностная обусловленность выбора форм образования, интегративность и расширение спектра видов деятельности; контекстность образования, направленного на креативность как развитие способности к самоизменению, самоопределению, преодолению традиционного взгляда. Одной из основных функций опережающего образования является компетентностная функция, предполагающая развитие целостного решения проблем в познании методом операционно-дидактической формы повышения квалификации педагогических кадров.

Для системы дидактической подготовки специалистов дошкольных учреждений в вузе характерна полифункциональность, выражающаяся во взаимозависимости в ее образовательной, воспитательной, развивающей, координирующей и интегрирующей функций. Их выделение условно, поскольку грани между обучением, воспитанием и развитием личности студента, а также интеграционными и координационными процессами в подготовке специалиста относительны [2]. Условная дифференциация функций дидактической подготовки необходима в целях эффективности теоретического анализа ее сущности и целесообразна для организации процесса обучения. Образовательная функция дидактической подготовки выражает ее направленность на овладение студентами фундаментальным знанием основ дидактической теории и формирование у них системы дидактических умений и навыков.

Теоретические и практические аспекты реализации образовательной функции дидактической подготовки предполагают изучение теории в контексте профессиональной деятельности будущих специалистов, что обеспечивает овладение студентами содержательно-процессуальными и организационно-методическими основами деятельности педагога дошкольного учреждения по обучению детей.

Воспитательная функция дидактической подготовки отражает ее позитивное влияние на формирование профессионально-значимых качеств личности, ее ценностно-нормативной системы, мотивов учебной и будущей профессиональной деятельности. В процессе овладения дидактической теорией и соответствующими умениями у студентов формируется ценностное отношение к дидактике как отрасли педагогической науки, потребность в обогащении системы дидактических умений и навыков, интерес, ответственное и творческое отношение к педагогической деятельности и процессу дидактической подготовки к ней, осознание себя ее субъектом.

В ходе дидактической подготовки, осуществляемой в контексте профессиональной деятельности, будущий специалист усваивает не только нормы компетентных предметных действий, но и нормы социальных поступков, отражающих ее ценностно-нормативную систему, ибо, как образно заметил А.А. Вербицкий, "специалист не воспитывается в социально стерильной учебной "пробирке..." [3]. Если предметное содержание будущей профессиональной деятельности обеспечивается материалом учебной дисциплины "Дидактика", то социальное "втягивается" в учебный процесс лишь при оптимальной организации индивидуальной, парной, групповой и коллективной форм деятельности студентов при ведущей роли коллективной.

Развивающая функция дидактической подготовки заключается в том, что овладение дидактическими знаниями и умениями органично связано с развитием профессионального

мышления, речи, педагогических способностей, позволяющих специалисту осуществлять творческий подход к организации образовательного процесса в дошкольном учреждении. Координирующая функция дидактической подготовки связана с ее направляющим влиянием на предстоящий процесс изучения студентами курсов дошкольной педагогики и частных методик, а также спецкурсов и спецсеминаров. Особая роль данной функции прослеживается при сравнительном анализе учебно-воспитательного процесса на разных факультетах педагогического вуза.

На большинстве факультетов курсы методик вооружают студентов знанием задач, принципов, содержания, форм и методов обучения по двум-трем определенным учебным предметам, в то время как на факультетах и отделениях педагогики и методики дошкольного образования изучаются пять-десять методик. Кроме того, изучаемые в вузе будущими педагогами дошкольных учреждений методики отличаются большей внутренней спецификой, нежели курсы методик в учебных планах других факультетов.

Следовательно, дидактическая подготовка будущего педагога является необходимым фундаментом всей его дальнейшей профессиональной подготовки. С реализацией координирующей роли дидактической подготовки связана ее интегрирующая функция. Обе функции обусловлены необходимостью междисциплинарного подхода к решению будущим специалистом дидактических проблем. Интегрирующая функция дидактической подготовки заключается в том, что процесс овладения дидактической теорией актуализирует, динамизирует, систематизирует и наполняет новым содержанием знания студентов, полученные ими при изучении курсов философии, социологии, психологии, теории воспитания и др. При этом, если координирующая функция дидактической подготовки студентов предполагает ее антиципирующее (предвосхищающее) влияние на предстоящие процессы, то в основе интегрирующей функции лежат рефлексия и аккумуляция достижений предшествующих и актуального этапов развития мотивационно-потребностной и операционно-действенной сфер личности. Реализация всех функций дидактической подготовки педагога осуществляется в ходе овладения студентами определенным содержанием. Научно обоснованный отбор содержания дидактической подготовки является одним из основных условий продуктивности поисков ее оптимизации.

Содержательный компонент дидактической подготовки представляет собой относительно самостоятельную область содержания педагогического образования, усвоение которой создает условия для овладения личностью дидактическими аспектами педагогической деятельности. Как известно, содержание образования формируется на трех уровнях: общего теоретического представления, учебного предмета и учебного материала [4]. Содержанием дидактической подготовки в нашей модели выступает педагогически адаптированная система дидактических знаний, способов педагогической деятельности, опыта ее творческого осуществления и ценностно-эмоциональных отношений, усвоение которой обеспечивает формирование дидактической культуры будущего специалиста. Содержанием дидактической подготовки, рассматриваемой в контексте профессионально-педагогической деятельности, является адаптированное с учетом семиотических и психолого-дидактических требований содержание дидактики как научной дисциплины, детерминированное спецификой профессиональной деятельности специалиста дошкольного учреждения.

Отбор содержания дидактической подготовки структурируется в логике развертывания учебного предмета "Дидактика" как предмета учебной, квазипрофессиональной (профессионально-подобной) и учебно-профессиональной деятельности. При этом требования со стороны будущей профессиональной деятельности являются системообразующими. В этом случае усвоение дидактических знаний осуществляется в контексте той деятельности, ориентировочной основой и средством регуляции которой они призваны выступать.

Основной единицей содержания дидактической подготовки в контексте профессиональной деятельности выступает педагогическая ситуация "во всей ее предметной и социальной неоднозначности и противоречивости" [5]. Формирование дидактической готовности педагога дошкольного образования требует включения учебной деятельности студентов в аналог будущего профессионального труда, представленный различными формами квазипрофессиональной деятельности. Моделирование содержания и динамики осваиваемой студентами профессионально-педагогической деятельности осуществляется посредством технологии контекстного обучения. Дидактическая подготовка с использованием форм и методов контекстного обучения характеризуется тем, что усвоение абстрактных по своей сути дидактических знаний "наложено на канву" профессионально-педагогической деятельности, что обеспечивает студенту их осмысление и усвоение как средства ее осуществления и регуляции.

Сущность контекстного обучения применительно к условиям дидактической подготовки педагога дошкольного образования состоит в деятельностной реконструкции профессиональной деятельности в ее предметном и социальном аспектах. Модель целостного содержания профессионально-педагогической деятельности представлена в контекстном обучении системой

профессиональных проблем, задач и функций, которые получают свое отражение в совокупности учебных, квазипрофессиональных и учебно-профессиональных заданий.

Создаваемые в учебном процессе модели выступают средством познания студентами оригинала - осваиваемой профессионально-педагогической деятельности - ее содержания, динамики, организационных форм, ценностей и норм, предметных задач. Совокупность дидактических задач, организационных форм и методов профессиональной деятельности специалистов, а также ситуаций их социально-психологического взаимодействия, регулируемого ценностно-нормативной системой педагогической деятельности, и составляет профессиональный контекст дидактической подготовки педагога дошкольного образования. Дидактическая подготовка педагогических кадров дошкольных учреждений осуществляется в целенаправленно моделируемой профессиональной среде на протяжении всего периода обучения в вузе и носит динамичный характер.

Этот процесс представляет собой последовательность пропедевтического, ориентационно-теоретического, формирующего и преобразующего этапов, каждый из которых сопровождается целесообразным воздействием на мотивационно-потребностную сферу личности будущего специалиста.

Деление целостного процесса дидактической подготовки педагога дошкольного образования на последовательные этапы условно, поскольку формирование дидактических умений будущего специалиста неизбежно сопровождается качественными преобразованиями системы его дидактических знаний и способствует становлению представлений о сущности дидактической подготовки, а достижение необходимого уровня усвоения дидактических знаний требует их применения в практической педагогической деятельности.

Каждому этапу дидактической подготовки соответствует определенная базовая форма организации деятельности студентов: учебная деятельность академического типа, квазипрофессиональная или учебно-профессиональная. Их последовательная трансформация и составляет основное содержание технологического компонента дидактической подготовки.

Проектирование дидактической подготовки студентов в контексте их будущей профессиональной деятельности требует конкретизации желаемых результатов этого процесса. Результативный компонент дидактической подготовки педагога дошкольного образования представляют взаимосвязанные аспекты дидактической готовности специалиста.

Дидактическую готовность педагога дошкольного образования составляет обусловленная необходимым уровнем его дидактической культуры способность к продуктивному дидактическому взаимодействию с детьми. Решаемым в ходе дидактической подготовки задачам соответствуют когнитивный, деятельностный, креативный и эмоционально-волевой аспекты дидактической готовности специалиста.

Дидактическая подготовка студентов, осуществляемая на основе представленной структурно-функциональной модели, призвана обеспечить повышение функциональной грамотности молодых специалистов в осуществлении дидактического взаимодействия с детьми дошкольного возраста.

Заключение. Разработано методическое обеспечение реализации модели и проведена ее опытно-экспериментальная проверка. Этапы предпринятого исследования будут конкретизированы в последующих публикациях.

СПИСОК ЛИТЕРАТУРЫ:

1. Лапчик М.П. Подготовка педагогических кадров в условиях информатизации образования учебное пособие/ Лапчик М.П.— М.: БИНОМ. Лаборатория знаний, 2013.— 182 с.
2. Грязнова Е.Д. Дистанционное обучение как средство педагогического воздействия в процессе профессиональной подготовки работников таможенных органов фия/ Грязнова Е.Д.— Владивосток: Владивостокский филиал Российской таможенной академии, 2011.— 160 с.
3. Абдуллина О.А. Общепедагогическая подготовка учителя в системе высшего педагогического образования. М.: Просвещение, 1990. 141 с.
4. Борисова Н.В. Педагогические особенности создания и внедрения системы активных методов обучения в институте повышения квалификации: Дис. ...канд. пед. наук. М, 1987. 334с.
5. Вербицкий А.А. Активное обучение в высшей школе: контекстный подход. М.: Высшая школа, 1991. 207 с.

УДК 364

КОНЦЕПЦИЯ СОЦИАЛЬНОЙ АДАПТАЦИИ СОТРУДНИКОВ СИЛОВЫХ МИНИСТЕРСТВ И ВЕДОМСТВ, УВОЛЕННЫХ В ЗАПАС

Михалев Юрий Валентинович, Хлюпин Владимир Алексеевич
Смольный университет Российской академии образования
Россия, Санкт-Петербург, Полюстровский пр., 59
e-mail: avtofakultet@mail.ru

Аннотация. В статье рассмотрены условия социальной адаптации сотрудников силовых министерств и ведомств. Дана характеристика основных условий социальной адаптации

военнослужащих, уволенных из Вооружённых Сил и пути решения возникающих проблем в современной экономической ситуации. Раскрыты несоответствия между правовыми гарантиями социальной защиты, поддержки и реальной помощи со стороны компетентных органов государства.

Ключевые слова: социальная адаптация; социальная защита людей; сотрудники силовых структур; военнослужащие, уволенные в запас; трудоустройство и переподготовка военнослужащих.

THE CONCEPT OF SOCIAL ADAPTATION OF EMPLOYEES OF POWER MINISTRIES AND DEPARTMENTS, RETIRED

Mikhalev Yuri., Hlyupin Vladimir
Smolny Institute of the Russian Academy of Education
Russia, St. Petersburg, Polyustrovskiy pr., 59
e-mail: avtofakultet@mail.ru

Abstract. The article describes the conditions of social adaptation of law enforcement ministries and departments. The characteristic of the basic conditions of social adaptation of servicemen discharged from the Armed Forces and ways of solving problems encountered in the current economic situation. Revealed discrepancies between the legal guarantees of social protection, support and real assistance by the competent authorities of the state.

Keywords: *social adaptation, social protection of people; law enforcement officers; military personnel transferred to the reserve; employment and retraining.*

Введение. Социальная адаптация в переводе (лат.) - приспособление к обществу, т.е. – приспособление человека к условиям социальной среды, способность изменяться самому в зависимости от изменения этих условий или при попадании в новую среду. Социальная адаптация — процесс интеграции человека в общество, в результате которого достигается формирование самосознания и ролевого поведения, способности к самоконтролю и самообслуживанию, адекватных связей с окружающими (…) [1]. Адаптация человека уже многие годы является основной проблемой многих областей научного знания. Раскрытие понятия адаптации помогает понять отношения человека с обществом, их взаимодействия. Разобраться в сущности адаптации весьма сложно, поскольку нет единого понятия, которое могло бы включать в себя ее полностью. Адаптация представляет собой одни из вполне реальных способов сохранения жизнеспособности человека не только в современном стремительно меняющемся мире, но и в будущем. В настоящее время социальный уклад меняется с все возрастающей скоростью. Человек, который не может приспособиться к этому оказывается никому не нужным и без средств к существованию. В особенности это важно для людей пенсионного возраста и инвалидов, т.к. им сложнее адаптироваться вследствие своих возможностей. Все это приводит к тому, что людям необходимо адаптироваться к быстро изменяющимся условиям жизни. Социальная адаптация предполагаеткак приспособление индивида к условиям жизнедеятельности (пассивная адаптация), так и активное целенаправленное их изменение (активная адаптация). Очевидно, что доминирование у человека активной адаптации обусловливает более успешное протекание социальной адаптации.

С выходом на пенсию начинается новый этап адаптации, который принципиально отличается по своей значимости. По мере старения снижаются приспособительные возможности любого организма - это общее объективное явление, характеризующееся угасанием важнейших жизненных функций - физических и психических. При изучении адаптации одним из наиболее актуальных вопросов является вопрос о соотношении адаптации и социализации. Процессы социализации и социальной адаптации тесно взаимосвязаны, так как отражают единый процесс взаимодействия личности и общества. В ходе социализации человек выступает как объект, воспринимающий, принимающий, усваивающий традиции, нормы, роли, созданные обществом. Социализация, в свою очередь, обеспечивает нормальное функционирование индивида в обществе. Социальная адаптация – это постоянный процесс активного приспособления индивида к условиям новой социальной среды;

Система социальной адаптации включает разные виды адаптивных процессов: производственная и профессиональная адаптация; бытовая (решает различные аспекты в формировании определённых навыков, установок, привычек, направленных к распорядку, традициям, существующим отношениям между людьми в коллективе, в группе вне связи со сферой производственной деятельности); досуговая (предполагает формирование установок, способностей к удовлетворению эстетических переживаний, стремление к поддержанию здоровья, физического совершенствования); политическая и экономическая; адаптация к формам общественного сознания (наука, религия, искусство, мораль и прочие); к природе и др.

В условиях построения гражданского общества большее внимание уделяется социальной защите людей и особенно тех, кто завершил службу в рядах государственных силовых структур Российской Федерации. Например, федеральные законы "О статусе военнослужащих", "О ветеранах" и др. Эти законы предусматривают для сотрудников, уволенных с государственной службы, права и льготы в сферах: здравоохранения и социального страхования; обеспечения жильем;

налогообложения и пользования транспортом; образования и культуры; трудоустройства и социального обеспечения.

Таким образом, эффективность решения проблем социальной адаптации сотрудников, уволенных с государственной службы, в большой степени зависит от их урегулирования нормами права. Только на основе нормативно-правового и организационного обеспечения возможно обеспечение прав и свобод сотрудников, предоставление им положенных льгот и эффективная защита их прав и интересов от любых нарушений. За последние годы в этом направлении предприняты активные действия: внедряются новые формы и технологии социальной работы с ветеранами силовых структур; перестроена пенсионная система; действует новый Трудовой кодекс; развивается система переподготовки и повышения квалификации сотрудников, уволенных с государственной службы. Рассмотрим существующие проблемы в области социальной адаптации военнослужащих, уволенных из Вооруженных Сил Российской Федерации. Среди проблем, с которыми сталкиваются военнослужащие, уволенные из Вооруженных Сил и члены их семей — вопросы занятости и профессиональной переподготовки, обеспечение жильем; низкий уровень социальной обеспеченности, падение экономической стабильности, психологическая адаптация, социальная реабилитация и т.д.

Система социальной защиты военнослужащих исторически складывалась как важнейший элемент государственной политики страны. В таком качестве она должна развиваться и впредь, активно взаимодействуя со всеми структурами власти и сферами жизни страны. Одной из самых серьезных проблем социальной адаптации является трудоустройство и переподготовка военнослужащих, уволенных из рядов Вооруженных Сил, так как она необходима прежде всего тем, кто не может найти себе работу после увольнения.

Результаты проведенных исследований [2] показали, что уволенные военнослужащие при формировании профессиональных перспектив ориентируются на такие сферы, как госслужба и управление (24%), армия и полиция (по 17%),. транспорт и связь (11 %); не определились с выбором сферы деятельности (30%). Особое место в решении вопросов трудоустройства занимает стремление ими пройти профессиональную переподготовку и овладеть профессией, гарантирующей трудоустройство (56%) Предпочитаемые профессии для переподготовки: менеджеры (31%), офисные работники и служба безопасности (по 17%).

Преимущественные критерии традиционны: высокий заработок, надежность трудоустройства и соответствие своим склонностям. При этом большинство (61%) не готовы оплатить переподготовку из личных средств, частично готовы - только 20%. Позитивный потенциал бывших военнослужащих необходимо поставить на службу стране, на развитие гражданского общества за счет успешного создания ряда новых общественных организаций — бывших военнослужащих, ветеранов Вооруженных Сил, молодежных, женских организаций. Бывшие военнослужащие – реальные носители патриотических начал. Это, как правило, трудоспособные люди, обладающие хорошей профессиональной подготовкой. Абсолютное большинство из них еще нуждается в активной профессиональной деятельности и способно, по своим деловым и нравственным качествам, принести значительную пользу обществу.

Социальную адаптацию пора перестать рассматривать только как средство для достижения конкретных целей снижения социального напряжения в среде бывших военнослужащих. Нужен более широкий взгляд на проблему, более глубокий анализ причин и следствий, задач и целей. Социально-психологическую адаптацию и реабилитацию военнослужащих, принимавших участие в боевых действиях, уволенных с военной службы затрудняют следующие факторы: их неконкурентоспособность в гражданском обществе на рынке труда; особенности личности, сформировавшейся в условиях военной службы;

изменение ролевого статуса (часто в сторону понижения); внутренние психологические барьеры, военная направленность их образования.

Уволенные с военной службы офицеры — это, как правило, трудоспособные люди, обладающие хорошей профессиональной подготовкой, содержание которой во многом родственно деятельности гражданских специалистов. Во время службы они получили опыт эксплуатации сложнейшей современной техники, решения задач в сфере операторской деятельности, в структурах управления, выполнение различных хозяйственных задач и т.д. Абсолютное большинство из них еще нуждается в активной профессиональной деятельности и способно, по свои деловым и нравственным качествам, принести значительную пользу обществу.

Однако, как показывает опыт, ситуация на рынке труда складывается для бывших военнослужащих далеко не благополучно. Многие учреждения, предприятия, отрасли хозяйствования вследствие продолжающего внешнеполитического и экономического кризиса стоят перед необходимостью значительного сокращения штата своих сотрудников. При нарастающем сокращении персонала (в особенности административно-руководящих должностей) предприятия не заинтересованы нанимать новых работников, а предпочитают оставлять своих специалистов, перемещая их по рабочим местам и вкладывая средства в их переподготовку. В этих условиях военнослужащим, уволенным в запас, не имеющим опыта трудовой деятельности в гражданской

сфере, а также отягощенных потерей личностного статуса и деформацией личности, вследствие участия в боевых действиях, особенно сложно найти работу. Хотелось бы обратить внимание на положительные аспекты и критерии, учитывая которые можно реально способствовать трудоустройству военнослужащих: профессиональная пригодность, в соответствии с военным профессиональным образованием, признанным в гражданской области и представляющим интерес для использования на гражданском рынке труда; общие особенности военнослужащих (ответственность и добросовестность, дисциплинированность и надежность, сознание долга и чувство ответственности, способность переносить, физические и психические нагрузки).

Концепция социальной адаптации военнослужащих и граждан, уволенных с военной службы. Исходной нормативной правовой основой Концепции является положение статьи 7 Конституции Российской Федерации, определяющее Российскую Федерацию социальным государством, политика которого направлена на создание условий, обеспечивающих достойную жизнь и свободное развитие человека [3].

Это конституционное положение ставит социальную защиту граждан центральной проблемой государства, предусматривает развитие системы социальных служб, декларирует гарантии социальной защиты.

Неотъемлемым компонентом системы социальной защиты является социальная адаптация военнослужащих, граждан, уволенных с военной службы, и членов их семей. Социальная адаптация военнослужащих — это деятельность органов государственной власти, военного управления, местного самоуправления, общественных объединений, должностных лиц и самих военнослужащих по подготовке и приспособлению к новым условиям жизни и деятельности после увольнения с военной службы.

Основные задачи социальной адаптации военнослужащих:

– планирование и осуществление мероприятий, направленных на смягчение социально-экономических и общественно-психологических последствий, связанных с увольнением военнослужащих и их социальной адаптацией;

– снижение социальной напряженности в местах размещения воинских формирований и проживания граждан, уволенных с военной службы; создание условий и возможностей для получения образования, переподготовки и трудоустройства;

– разработка предложений по совершенствованию законодательства о правах, льготах и социальных гарантиях военнослужащих, граждан, уволенных с военной службы, и членов их семей; совершенствование механизмов и институтов социальной адаптации военнослужащих.

Результаты исследований в области профориентации и переподготовки бывших военнослужащих позволяют заключить, что исключительно важно добиваться максимального сокращения того периода времени, в течение которого увольняемый (а затем и уволенный) проходит путь от завершения военной службы до работодателя.

Это позволит строго выдерживать общую линию на снижение затратности мер поддержки увольняемых по их переходу в условия гражданской жизни.

В то же время, ощущается явная несбалансированность процессов реформирования Вооруженных Сил, других войск и их ресурсного обеспечения в условиях несформировавшегося рынка труда, что снижает возможности реализации социальной и профессиональной адаптации бывших военнослужащих.

По-прежнему, остро стоит задача переориентации с настраивания увольняемого офицера (прапорщика, мичмана) на фундаментальное переобучение, на предварительное его профессиональное консультирование, на психологическую подготовку увольняемого к действиям на современном рынке труда.

Существующая в настоящее время практика не способствует развитию собственной активности и нацеленности уволенных на заблаговременный поиск работы и успешное трудоустройство. Возможность бесплатной профессиональной переподготовки увольняемых и уволенных с военной службы становится в современных экономических условиях все более проблематичной.

Заключение.

Таким образом, в представленном материале дана характеристика основных условий социальной адаптации военнослужащих, уволенных из Вооружённых Сил и пути решения возникающих проблем в современной экономической ситуации. Раскрыты несоответствия между правовыми гарантиями социальной защиты, поддержки и реальной помощи со стороны компетентных органов государства.

СПИСОК ЛИТЕРАТУРЫ:

1. Альмуханова А. Б. и др. Большая психологическая энциклопедия М.: Эксмо, 2007. 542 с.
2. Непрерывное образование взрослых: Материалы Международного форума / Отв.ред. В.В. Беличенко, С.В. Кривых, В.Я. Никитин. -СПб.: ИНОВ, 2015.-350 с.
3. Конституция Российской Федерации, 1993 г.

УДК 004.056.5

МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ ЗАЩИЩЕННОСТИ ДАННЫХ ЭЛЕКТРОННОЙИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ УНИВЕРСИТЕТА

Соколов Сергей Сергеевич, Ныркov Анатолий Павлович, Ковальногова Надежда Михайловна,
Мамунц Давид Гарикович, Пастушок Елена Михайловна
ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»
Россия, Санкт-Петербург, ул. Двинская, 5/7
e-mail: iapbgks@bk.ru

Аннотация. В статье рассматривается задача обеспечения информационной защищенности данных электронной информационно-образовательной среды университета. В части защиты рассматривается информация ограниченного доступа, не относящаяся к государственной тайне, включающая авторское право, персональные данные, коммерческую и другую информацию.

Ключевые слова: *электронная информационно-образовательная среда; безопасность данных; защита персональных данных.*

THE METHODS OF PROVIDING INFORMATION SEQURITY OF THE UNIVERSITY ELECTRONIC DATAINFORMATION AND EDUCATIONAL ENVIRONMENT

Sokolov Sergey, Nyrkov Anatoliy, Kovalnogova Nadegda, Mamunts David, Pastushok Elena
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya str, St. Petersburg, Russia
e-mail: iapbgks@bk.ru

Abstract. In this article presented the problem of ensuring information security of the electronic information and educational environment of the university. In the part of protection, information of limited access that is not related to state secrets, including copyright, personal data, commercial and other information.

Keywords: *electronic information and educational environment; data security; protection of personal information.*

На сегодняшний день электронное обучение (далее – ЭО) и дистанционные образовательные технологии (далее – ДОТ) широко используются в мировой практике. В России предпосылки к использованию ЭО и ДОТ при реализации образовательных программ регламентированы рядом нормативно-правовых документов, в частности Федеральным законом от 09.12.2012 № 273-ФЗ «Об образовании в Российской Федерации». При реализации образовательных программ Университетом используются различные образовательные технологии, в том числе дистанционные образовательные технологии, электронное обучение. Для применения ЭО и ДОТ Университет должен создать условия для функционирования электронной информационно-образовательной среды (далее – ЭИОС). Электронная информационно-образовательная среда ВУЗа включает в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств и обеспечивает освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся [1, 2]. Это подразумевает под собой такие задачи ЭИОС, как обеспечение круглосуточного доступа обучающихся к содержанию учебных дисциплин посредством сети Интернет; создание условий для обеспечения обучающимся возможности самостоятельной подготовки к занятиям, выполнению заданий, подготовки к аттестации; организация электронного документооборота УК, автоматизация процесса управления учебным процессом и многое другое. При этом одна из важнейших задач – обеспечение информационной безопасности этих технологических процессов ЭИОС. Рассмотрим некоторые обязательные методы обеспечения защищенности данных при работе в ЭИОС/

Настройка методов аутентификации

В ЭИОС существует несколько способов аутентификации пользователей:

– ручная регистрация;
– внешняя база данных;
– самостоятельная регистрация по электронной почте.

Ручная регистрация предполагает подачу заявки через форму подачи заявки и последующую регистрацию сотрудником ЭИОС. Такой вид регистрации обязателен для проверки данных по заявке и предоставлению доступа к ЭИОС.

Регистрация через внешнюю базу данных предполагает синхронизацию с некоторой базой данных, которая регулярно обновляется, для создания новых пользователей в ЭИОС.

Самостоятельная регистрация по электронной почте позволяет упростить и ускорить процесс регистрации пользователей в ЭИОС. Однако, преподаватель, при самостоятельной регистрации, не

сможет назначить себе права преподавателя. Для этого ему придется обратиться к сотруднику или администратору ЭИОС [3].

Установка настроек безопасности ЭИОС

В ЭИОС предусмотрены настройки безопасности, которые работают в совокупности с настройками безопасности сервера. ЭИОС позволяет уведомлять о внештатных ситуациях, возникающих при входе в систему или при попытках нарушить безопасность ЭИОС. Уведомления о нарушении безопасности приходят на почту администратору ЭИОС.

Настройки безопасности также позволяют использовать защищенный протокол интернет-соединения для обмена информацией.

В настройках безопасности ЭИОС необходимо проверять все настройки и правильность их установки. На странице безопасности необходимо настроить такие параметры как:

– защита логинов (отсутствие подсказок на странице восстановления паролей, восстановление происходит только через электронную почту);
– принуждение входа в систему (обязательный вход для просмотра содержимого ЭИОС);
– видимые роли (отображает только те роли, которые будут настроены администратором);
– максимальный размер загружаемого файла;
– квота пользователя (максимальный размер хранилища личных файлов пользователя);
– политика паролей;
– блокировка ip- адресов (белый и черный лист ip – адресов).

Установка значений по умолчанию для некоторых функций ЭИОС

При создании информационных активов в ЭИОС имеются обязательные для заполнения поля, а есть поля, которые заполняются автоматически по умолчанию.

Обязательными полями для заполнения являются полное и короткое название электронного курса.

Поля, заполняемые автоматически:

– видимость курса (не позволяет видеть содержимое курса обучающимися до момента опубликования);
– начало курса (ставится день создания курса);
– способ записи на курс – зачисление вручную (позволяет преподавателю самостоятельно выбирать и записываться обучающихся на курс);
– количество разделов курса (всегда ставится значение 3, его можно изменить).
– При регистрации пользователей также существуют поля, которые заполняются по умолчанию, автоматически:
– отображение адреса электронной почты другим пользователям ЭО;
– город;
– часовой пояс;
– предпочитаемая тема оформления всей ЭИОС;
– язык.

Настройка внешнего вида

Так как оформление играет немаловажную роль в освоении навигации и восприятии информации в ЭИОС, внешнему виду ЭИОС должно отводиться особое внимание.

Для настройки внешнего вида в ЭИОС существуют темы оформления, которые позволяют менять внешнее обрамление всех элементов навигации, шрифты, цвета и т.д.

При обновлении платформы рекомендуется обновлять тему оформления ЭИОС в целом. Так как тема предыдущей версии платформы может отображаться некорректно. При настройке темы необходимо учитывать удобство использования тех или иных элементов, а также простоту восприятия.

Для повышения функциональности ЭИОС рекомендуется раз в полгода проводить мониторинг новых плагинов, которые появляются на официальной странице разработчика платформы, помня при этом об обеспечении информационной безопасности в системе ЭИОС [4].

Плагины позволяют расширять возможности ЭИОС для администрирования ЭИОС, для создания ЭК, для управления обучающимися и контроля выполнения ЭК. Плагины дают возможности создавать новые элементы ЭК, которые разнообразят представление методического обеспечения дисциплины в ЭИОС.

Назначение прав пользователю

Для разных категорий пользователей в ЭИОС существуют различные роли. При регистрации любого обучающегося или преподавателя, по умолчанию присваивается роль «Обучающийся». Но если проходит регистрация преподавателя, то ему, после создания профиля, выдаются права «Преподаватель».В рамках ЭК также имеются различные права на управление ЭК:

– управляющий;
– преподаватель;

– обучающийся;
– ассистент с право редактирования.

Пользователь с правами «Управляющий» имеет право на полный доступ к ЭК. Он может просматривать результаты обучающийся, редактировать все элементы ЭК, настраивать, добавлять и удалять их. Управляющий определяет порядок прохождения ЭК, какие ограничения накладываются на те или иные элементы курса, управлять участниками ЭК и т.д.

Пользователь с правами «Преподаватель» имеет те же самые права, что и Управляющий, кроме возможности удалять ЭК, настраивать способы записи на курс, а также изменять права участников ЭК.

Пользователь с правами «Обучающийся» имеет право только на просмотр элементов ЭК, выполнение заданий и тестовых заданий. При наличии в ЭК форумов или чатов, обучающийся имеет право на участие в форумах и чатах.

Пользователь с правами «Ассистент с правом редактирования» имеет право на редактирование элементов ЭК, их настройку. Участник курса с такими правами не имеют право на управление участниками курса, и на другие функции, которые имеются у преподавателя.

Контроль производительности сервера и базы данных электронной оболочки

Для успешной работы ЭИОС необходимо постоянно контролировать аппаратное и программное состояние сервера и его производительность. Контролем производительности и состояния программно-аппаратного обеспечения сервера занимается Администратор ЭИОС.

Программное обеспечение на сервере должно быть максимально актуальным и обновляться не реже один раза в три месяца. Для контроля производительности ресурсов, направленных на поддержание работоспособности ЭИОС, на сервере должно быть специальное программное обеспечение – монитор. При нехватке ресурсов на сервере необходимо выяснить причину нехватки и при необходимости либо увеличить вычислительную мощность сервера, либо проверить ресурсозатратность служб [5].

Техническое обслуживание аппаратной составляющей сервера ЭИОС должно проводиться не реже один раза в год. В техническое обслуживание аппаратной составляющей входит чистка компонентов сервера, поддержание комфортной температуры в помещении. А также обновление аппаратных составляющих при необходимости повышения производительности сервера.

Производительность базы данных зависит от обновлений платформы ЭИОС. Если платформа требует обновления формата таблиц в базе данных для повышения производительности, то это действие необходимо выполнить. В ЭИОС предусмотрена таблица производительности, в которой появляются предупреждения о наличии таблиц в устаревшем формате. Проверять наличие таких уведомлений необходимо один раз в полгода.

В заключение отметим. На сегодняшний день перед российской системой образования стоит ряд важных проблем, среди которых следует выделить необходимость повышения качества и обеспечения равных возможностей доступа к образовательным ресурсам и сервисам всех категорий граждан. Создание информационной среды, удовлетворяющей потребности всех слоев общества в получении широкого спектра образовательных услуг, а также формирование механизмов и необходимых условий для внедрения достижений информационных технологий в повседневную образовательную и научную практику является ключевой задачей на пути перехода к информационному обществу. Обеспечение информационной безопасности ЭИОС образовательного учреждения очень актуально: количество угроз растет с каждым днем, изменяется количество компонентов ЭИОС, устаревает программное обеспечение платформ и т.д.

Безопасность данных компонентов ЭИОС обеспечивается собственным программно-аппаратным обеспечением каждого отдельного компонента ЭИОС и рядом организационно-технических мер. Основой защиты информации от несанкционированного доступа является реализация принципов контроля доступа к ресурсам. Обеспечение корректности реализации разграничительной политики доступа к ресурсам невозможно без корректной идентификации пользователей. Применение модели идентификации пользователей позволяет контролировать использование компонентов ЭИОС и анализировать состояние защищенности ЭИОС. Но надо помнить и то, что большая часть угроз информационной безопасности организаций, в том числе и образовательных учреждений, возникает не извне, а изнутри. Поэтому актуальным является серьезное отношение к методам противодействия социальному инжинирингу [6-8].

СПИСОК ЛИТЕРАТУРЫ

1. Ныркова А.П. Применение электронного обучения и дистанционных образовательных технологий в ГУМРФ имени адмирала С.О. Макарова / А. П. Ныркова, С. С. Соколов, Н. М. Ковальногова // «Перспективные направления развития отечественных информационных технологий»: материалы II межрегиональной научно-практической конференции. Севастопольский государственный университет; науч. ред. Б.В. Соколов. Севастополь, 2016. – С. 53-54.
2. Kovalnogova, N. Applying E-learning and Distance Learning Technologies in Modern University Complex / N. Kovalnogova, S. Sokolov, A. Nyrkov, S. Chernyi // Asian Journal of Applied Sciences, Volume 3, Issue 6, 2015. – Pp. 790-793.
3. Kovalnogova N.M. Model of user identification of electronic informational-educational environment / N. M. Kovalnogova, S. S. Sokolov, A. P. Nyrkov // IOP Conf. Series: Materials Science and Engineering 124 (2016) 012066, 2016. doi:10.1088/1757-899X/124/1/012066/

4. Люльченко А.Н. Модель системы обеспечения информационной безопасности на транспорте / А. Н. Люльченко, А. П. Нырков, В. Г. Швед // Вестник государственного университета морского и речного флота имени адмирала С.О. Макарова, № 5 (33), 2015. – С. 184 – 193.
5. Nyrkov A.P. Algorithmic Support of Optimization of Multicast Data Transmission in Networks with Dynamic Routing / A. P. Nyrkov, S. S. Sokolov, A. S. Belousov // Modern Applied Science. – Vol. 9. – No. 5, 2015. – Pp. 162 – 176. doi:10.5539/mas.v9n5p162.
6. Теплов Э.П. Гуманитарные аспекты информационной безопасности: методология и методика поиска истины, построения доказательства и защиты от манипуляций / Э. П. Теплов, Ю. А. Гатчин, А. П. Нырков, В. В. Сухостат. – СПб: Университет ИТМО, 2016. – 120 с.
7. Теплов Э.П. Гуманитарные аспекты информационной безопасности: основные понятия, логические основы и операции / Э. П. Теплов, Ю. А. Гатчин, А. П. Нырков, А. Г. Коробейников, В. В. Сухостат. – СПб: Университет ИТМО, 2016. – 122 с.
8. Теплов Э.П. Гуманитарные аспекты информационной безопасности: получение, анализ и оценка деловой информации / Э. П. Теплов, А. П. Нырков, А. В. Башмаков, Е. К. Брагина. – СПб.: Издательский Дом «Афина», 2016. – 160 с.

УДК 371.39

ПЕДАГОГИЧЕСКИЕ И ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОГО ТЕСТИРОВАНИЯ НА РАЗНЫХ СТАДИЯХ ОБУЧЕНИЯ ДИСЦИПЛИНЕ

Титова Юлияна Францевна
Смольный институт Российской академии образования
Кафедра информационных систем
Россия, Санкт-Петербург, Полюстровский пр., 59
e-mail: titova-stud@yandex.ru

Аннотация. В статье рассмотрены педагогические и технологические аспекты использования компьютерного тестирования на разных стадиях обучения дисциплине. Дана типология тестовых вопросов. Рассмотрен малоиспользуемый, но перспективный вид тестовых вопросов «вычисляемый». Описаны возможности использования компьютерных тестов, как на стадии обучения, так и на стадии контроля. Рассмотрены особенности настройки компьютерного теста в LMSMoodle в зависимости от педагогических целей.

Ключевые слова: *LMS-система; Moodle; методика; электронное обучение; тестовый вопрос; вычисляемый вопрос; тест, типология компьютерных тестов.*

PEDAGOGICAL AND TECHNOLOGICAL ASPECTS OF THE USE OF COMPUTER-BASED TESTING AT DIFFERENT STAGES OF LEARNING THE DISCIPLINE

Titova Yuliayna
Smolny Institute of the Russian Academy of Education
Department of information systems
Russia, Sankt-Peterburg, Polyustrovskiy pr., 59
e-mail: titova-stud@yandex.ru

Abstract. The article deals with pedagogical and technological aspects of the use of computer-based testing at different stages of learning the discipline. Given typology test questions. Considered under-utilized, but promising form of test questions "calculated". The possibilities of using computer tests, during learning and during supervision. The features of the settings of the computer test in LMS Moodle, depending on pedagogical purposes.

Keywords: *LMS; Moodle; methodology; e-learning; the test question; a numerical question given test, types of computer tests.*

Все большее количество вузов внедряет системы управления образовательным контентом (LMS-системы) в учебный процесс. Одна из них - свободно распространяемая среда LMS Moodle - предоставляет богатые возможности организации электронного обучения: элементы для представления учебных материалов в виде файлов (текстовых, презентаций, видео и пр.), интерактивные элементы (рабочие тетради, форумы, чаты, опросы, задания), средства для создания контрольно-измерительных материалов (базы тестовых вопросов), средства анализа результатов обучения с использованием шкал. Как правило, среду с успехом используют наиболее передовые преподаватели, которые довольно хорошо владеют информационными технологиями, имеют интерес к электронным формам обучения и способны самостоятельно освоить технологии работы в среде LMS. Хуже ситуация с основным контингентом преподавателей со слабой компьютерной подготовкой и отсутствием мотивации создания и применения электронных средств обучения [1]. Если государство и администрация вузов найдут формы повышения такой мотивации, то тогда на повестку дня встанут вопросы разработки педагогических методик использования возможностей LMS-систем в обучении. На сегодняшний день можно констатировать факт, что до сих пор отсутствует педагогическое обоснование правомочности, эффективности использования разнообразных возможностей LMS при обучении. Поэтому преподаватели используют элементы электронного обучения так, как умеют, и насколько хватает их знаний об используемой среде LMS. Однако при неумелом использовании возможностей среды можно получить отрицательный педагогический

результат. Одним их таких отрицательных примеров является использование в тестах вопросов типа «множественный выбор», когда испытуемому задают вопрос и на выбор предлагаются варианты ответов. Даже при отсутствии знаний по дисциплине путем угадывания можно получить зачетный результат. В связи с этим от вопросов такого типа уже стали отказываться и на уровне государственного тестирования, а именно в тестах ЕГЭ по естественнонаучным дисциплинам. Для педагогически правильного использования тестирования в учебном процессе необходимо не только объяснять технологические возможности использования отдельных элементов среды, но и давать педагогическое обоснование, на какой стадии учебного процесса и в каком виде их применять. При этом надо учесть тот факт, что для большинства преподавателей в силу многих причин освоение среды LMS представляет большие трудности, и поэтому курсы по технологии работы в среде и педагогическим методикам использования среды надо проводить от простого к сложному.

В учебном процессе, как известно, выделяется учебная стадия и контролирующая стадия. С точки зрения электронного обучения предполагается, что студенту будут представлены учебные материалы в электронной форме. В самом простом случае это файл с конспектом лекции и файлы с примерами выполнения практических заданий. Такие ресурсы, по сути, являются заменой бумажных учебников. Но как проконтролировать, насколько правильно усвоил материал студент? Для этого среда LMS предоставляет возможность проверки знаний в форме тестирования.

Для организации компьютерного тестирования в современных LMS необходимо организовать базу вопросов и разработать тесты. Будем называть тестом совокупность вопросов, специальным образом отобранную из базы, на которые должен ответить обучающийся в соответствии с поставленной педагогом целью обучения. Здесь кроется первая проблема – многие преподаватели не видят разницы между тестом и тестовыми вопросами. В печатных учебных изданиях последнее время довольно часто стали встречаться тесты как формы проверки знаний. Эти тесты располагаются после параграфа или главы, и основной их целью является проверка знаний конкретно по данной теме. И вот по аналогии с таким «бумажным» тестом - преподаватели не отделяют тестовый вопрос как самостоятельную единицу. Это на бумаге тестовый вопрос встретится только один раз в одном тесте. Но когда речь идет об электронной среде и базе тестовых вопросов, их функция существенно расширяется. Как сказано выше, из тестовых вопросов можно составлять разные тесты, например, для проверки знаний по теме одной лекции, тест проверки знаний по теме программы, тесты для рубежного контроля и для итогового контроля. Электронный вопрос может присутствовать во всех этих тестах.

В LMS Moodle предлагается несколько типов вопросов, разной трудоемкости и технологической сложности. Наиболее простыми и в том, и в другом плане являются вопросы со множественным выбором, о которых говорилось выше. Большинство преподавателей и методистов знают только такую форму тестового вопроса, и поэтому она является самой распространенной в вузовской среде. Даже ФОСы требуют создавать, используя только эту форму вопроса. По этим причинам они наиболее часто используются преподавателями. Основная трудоемкость создания таких вопросов заключается в подборе неправильных ответов, которые бы «выглядели» как правильные. Негативной стороной является возможность подбора ответа студентом, т.к. зачастую довольно просто «отсечь» неправильные ответы. Именно поэтому такие вопросы должны иметь ограниченную применимость. Например, в тех случаях, когда вопросы заранее студенту не известны, что имеет место при официальном тестировании. Тем не менее, совсем отказываться от них не разумно. Вопросы такого типа можно успешно использовать для контроля усвоения терминологии курса, для проверки знания дат, фамилий, названий чего-либо. Для проверки терминологии общая структура вопроса может выглядеть следующим образом. В теле вопроса дается формулировка определения термина и ставится вопрос «О каком термине идет речь?». В ответе в качестве множественного выбора приводятся термины курса, из которых надо выбрать один. Ответов на выбор надо предложить достаточное количество (желательно более 6), чтобы уменьшить вероятность выбора правильного ответа случайным образом. В этом случае не надо придумывать неправильные ответы, и решается педагогическая задача усвоения терминологии.

Другой, более глубокий уровень тестовых вопросов представляют вопросы с коротким ответом. Технология создания таких вопросов не очень сложна и хорошо описана – надо составить формулировку вопроса, на который студенты должны ввести в качестве ответа короткую фразу произвольным образом, обычно 1-3 слова. Трудоемкость разработки такого вопроса заключается в подборе формулировок правильных ответов и описании их. Значительную помощь в составлении вопроса оказывает использование технологии подстановочных знаков, что позволяет отбросить возможные окончания слов. Возможные варианты ответов можно определить в ходе анализа ответов студентов на вопрос и тем самым при необходимости откорректировать его. Педагогическая ценность таких вопросов гораздо выше, потому что студент должен понять, о чем речь, найти и прочитать нужное место в учебнике, а также сформулировать кратко ответ. Кроме этого решается задача правильного написания слов (в т.ч. и терминов). Здесь уже нет готовых ответов, чтобы методом подбора найти правильный. Однако надо констатировать факт, что в учебном процессе эти вопросы используются очень мало, особенно преподавателями некомпьютерных дисциплин.

В современных LMS также присутствует форма тестового вопроса «на сравнение». В таких тестах испытуемому предлагается к заданным формулировкам (вопросам) подобрать правильные ответы и ограниченного набора. Количество вопросов и ответов может не совпадать. На разные вопросы может быть один и тот же ответ. В какой-то мере этот тип вопроса поход на вопрос со множественным выбором, но у него больше аспектов использования. Например, с помощью таких вопросов можно попросить установить правильную последовательность расположения чего-либо (дат, исторических событий, действий в алгоритме и пр.). Технология создания такого теста очень проста – надо описать все формулировки и указать правильный ответ к каждой. Неправильные ответы тоже гораздо проще придумать.

И, наконец, хочется остановиться на вычисляемых вопросах. Это на настоящий момент практически неиспользуемая форма тестовых вопросов. По своей сути такой вопрос позволяет организовать решение некой вычислительной задачи, в которой традиционно заданы исходные данные и требуется получить результат с использованием одной или нескольких формул. Вычисляемые задачи используются при обучении экономическим, естественнонаучным, в том числе и компьютерным, дисциплинам. В традиционной вычисляемой задаче формулировка включает описание ситуации, набор известных исходных данных и вопрос, что требуется найти. Задача решается в одно или несколько действий. На каждом этапе вычислений применяется формула, связывающая известные и неизвестные величины. В большинстве случаев набор исходных данных является минимально необходимым, т.е. все исходные данные при решении так или иначе должны быть использованы. В любой дисциплине можно выделить типовые задачи, выстроить их в методической последовательности освоения. И самая большая проблема – это научить студентов видеть в формулировке некой конкретной задачи целую категорию, и применять типовой для этой категории метод. Решить эту проблему можно в том числе и многократным решением типовых задач, что не позволяет делать современный процесс обучения. Электронный вычисляемый вопрос позволяет на основе одной формулировки сгенерировать целую категорию типовых задач. Во время тестирования к типовой формулировке добавляется случайный набор исходных данных, что делает конкретную задачу уникальной для каждого тестируемого, чем обеспечивается индивидуализация тестирования и невозможность механического запоминания ответа. Наличие электронных вычисляемых вопросов позволит студенту самостоятельно тренироваться решать задачи в том объеме, пока он уверенно не освоит категории типовых задач. И степень его умений будет зависеть только от его прилежности, способностей и упорства.

Создание вычисляемого вопроса включает описание типовой формулировки задачи, программирование формулы правильного ответа и создание наборов исходных данных. Сама формулировка – это, по сути, обобщенное описание некоторого класса однотипных задач, наборы исходных данных позволяют сформировать множество задач с одинаковыми формулировками и с разными исходными данными. Для создания наборов данных в LMS-среде предусмотрена технология автоматической генерации чисел в заданном диапазоне с заданной погрешностью, что снижает трудоемкость создания вопросов, что избавляет преподавателя от придумывания наборов данных.

Проблемы использования вычисляемых вопросов заключаются в том, что, во-первых, не понятно, как преподаватели узнают о том, что такая форма вопросов есть, во-вторых, кто их научит создавать такие вопросы, и в-третьих, что технология их создания предполагает, хоть и несложное, но программирование формулы. Администраторы системы во многих вузах ограничиваются чисто администраторскими функциями, а именно создание учетных записей, ведение списка групп, общая настройка системы. В их функции не входит исследование возможностей системы и обучение преподавателей, а также методическое обоснование использования элементов системы в учебном процессе. Именно поэтому при организации системы электронного обучения должен быть предусмотрен методист, решающий именно такие методические задачи. Проблема программирования формул решается тем, что, если в дисциплине есть вычислительные задачи, которые предполагают какой-никакой алгоритм решения, значит, и преподаватель способен освоить несложные элементы программирования.

У электронных вычисляемых вопросов есть и более важная функция, чем просто организация решения традиционной вычислительной задачи. Повысить обучающий эффект можно также за счет использования разработки так называемых комплексных задач. В данном контексте под комплексной задачей понимается описание в тестовом вопросе ситуации, по которой можно задать несколько вопросов, использующих для ответа разные формулы. Для такой ситуации задается набор исходных данных, необходимый для ответа на все вопросы. С точки зрения одного конкретного вопроса к ситуации этот набор данных будет избыточным. Такой подход позволяет получить вместо одного вопроса несколько тестовых вопросов с использованием одного и того же набора данных. Кроме этого, в среде есть также возможность отображения в теле вопроса исходных данных, которые сами получены по некоторой формуле, что позволяет использовать тот же набор данных для формулировки обратных задач и тем самым еще большего расширения круга вопросов по описанной ситуации. Допустим, у нас есть 3 исходных величины (a, b, c), по которым можно вычислить 2 других

величины по некоторым формулам, например, d(a, b) и f(b, c). По заданному набору данных (a, b, c) можно создать вопросы с такими формулировками (неполный перечень):

дано a, b, c найти d; - это прямая задача с одним действием
дано a, b, c найти f; - это прямая задача с одним действием
дано b, c, d найти a; - это обратная задача с одним действием
дано f, c, d найти a; - это обратная задача с двумя действиями
дано f, b, d найти a; - это обратная задача с одним действием
дано f, b, d найти c; - это обратная задача с одним действием
и т.д.

Понятно, что увеличение количества исходных данных в геометрической прогрессии расширяет круг вопросов, которые можно задать. Использование комплексных ситуаций в тестовых вычислительных задачах формирует у студента интегрированные знания по курсу. Такие комплексные задачи намного ближе к реальным ситуациям. Ведь в жизни и профессиональной деятельности именно человек из множества величин должен понять, какие нужны для ответа на тот или иной вопрос.

Ниже приводится пример комплексной ситуации в курсе «Имитационное моделирование». На рисунке приводится описание ситуации по простейшей модели системы массового обслуживания с очередью и 1-м узлом обслуживания из n каналов, построенной в среде AnyLogic. Вместо чисел, отображаемых при проигрывании модели, указаны параметры. При создании тестового вопроса часть этих параметров задаются в наборе данных, другие вычисляются по формулам, которые скрыты от студентов.

Обобщенная формулировка ситуации: На рисунке (рис. 1) представлена функциональная модель системы массового обслуживания (СМО) в некий текущий момент времени. Известно, что за единицу времени в СМО поступает в среднем {x} заявок. Каждая заявка обслуживается каналом обслуживания в среднем {y} единиц времени. Считаем, что поток заявок и поток обслуживания являются простейшими.

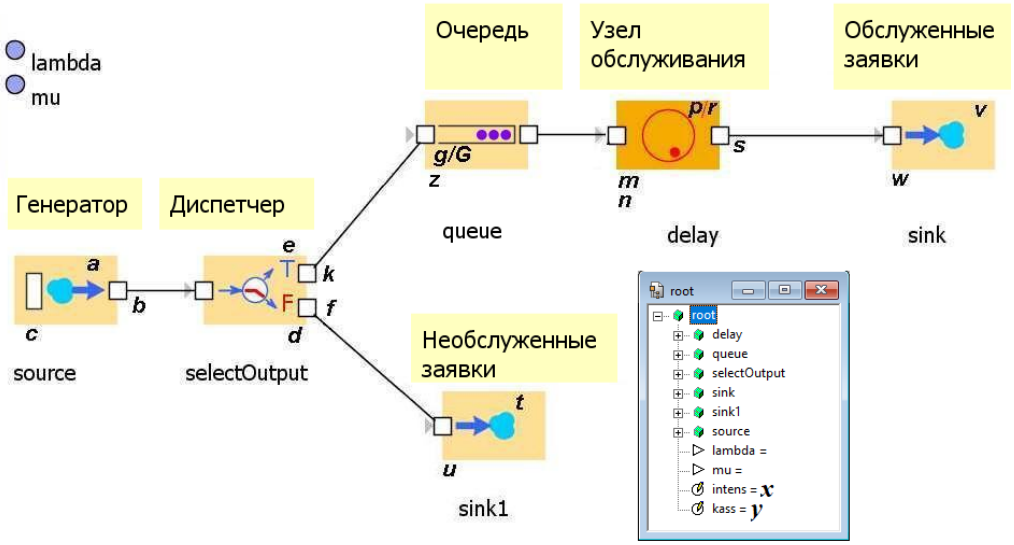


Рис. 1. Система массового обслуживания в среде Anylogic 5

По описанной ситуации можно задать порядка 80 разнообразных вопросов. В простейших вопросах проверяется, понимают ли студенты, какие показатели отражаются на модели. В более сложных вопросах студенты должны вычислить другие показатели СМО, не отраженные в модели.

Как известно, решение задач – это один из основных методов усвоения теории. Зачастую аудиторного учебного времени не хватает, для прорешивания всевозможных вариантов постановки задач. Поэтому использование вычисляемых вопросов позволяет продолжить обучение в режиме самостоятельной работы. По мнению автора, вычисляемые вопросы должны составлять основную часть фонда оценочных средств. Это согласуется с современной концепцией образования, направленной на формирование у студентов бакалавриата прикладных навыков. Поэтому необходимо организовать обучение преподавателей, в первую очередь экономических дисциплин, технологии создания таких вопросов в рамках курсов повышения квалификации. При обучении надо обязательно касаться и технологической и педагогической составляющих, что могли бы сделать в большей степени преподаватели компьютерных технологий, а не системные администраторы.

Коснемся далее типологии тестов, которые можно использовать в учебном процессе. Следует заметить, что создание тестов с разными настройками на основе одной и той же базы вопросов позволяет решить различные педагогические задачи в процессе обучения.

Так можно предложить следующие типы тестов:

– тест входного контроля – предполагает проверку остаточных знаний по изученным ранее дисциплинам. Такой тест должен использовать вопросы из изученных ранее дисциплин. В LMS это достигается экспортом/импортом вопросов из одной дисциплины в другую.

– тест для самостоятельного тестирования по теме (для самоподготовки, для самопроверки) – включает вопросы одной из тем курса, предназначен для подготовки к контрольному тестированию.

– контрольный тест по теме – обеспечивает контроль усвоения знаний по одной из тем курса.

– рубежный тест – содержит вопросы по нескольким последовательным темам и проводится 1-2 раза в семестр в зависимости от объема изучаемой дисциплины.

– пробный тест итогового контроля – включает вопросы по всем темам и предназначен для подготовки к итоговому тестированию по дисциплине.

– итоговый тест по дисциплине – для итоговой проверки знаний.

Использование этих видов тестов не вызывает сомнения. Дополним этот перечень рядом других типов, которые также можно использовать в учебном процессе.

Как промежуточный этап в процессе усвоения теоретических знаний по отдельной теме можно использовать тест, названный автором «Работа с учебником». В этот тест вопросы включаются в логической последовательности предъявления учебного материала. При этом порядок вопросов не меняется. Для прохождения этого теста достаточно 1-й попытки (не более 3-х), и студенту рекомендуется проходить этот тест вместе с чтением конспекта. Такая форма учебной работы обеспечивает и последовательное прочтение учебного материала, а не хаотичный поиск по учебнику ответа на тестовый вопрос, если вопросы включены в тест случайным образом, и первичное ознакомление с базой вопросов. При выстраивании траектории обучения надо обеспечить переход к тестам для самостоятельного тестирования только после прохождения теста «Работа с учебником».

Другой тип тестов можно назвать «Учебный тест». Он некоторым образом моделирует процесс проведения практического занятия, на котором преподаватель со студентами рассматривает примеры решения задач по теме. Как правило, на занятии преподаватель предлагает методически подобранную систему задач, ориентированных на применение определенного вычислительного аппарата и на получение представления о типологии задач по данной теме. Преподаватель руководит процессом решения задач, показывает примеры решения и пр. Отталкиваясь от этой технологии можно сформулировать основные принципы построения учебного теста.

Тест должен содержать вопросы в основном вычисляемого типа.

Вопросы в тесте располагаются в строго логическом неизменяемом порядке.

Тест содержит вопросы-примеры и вопросы-задачи. В вопросах-примерах дается формулировка задачи, приводится пример решения аналогичной задачи с другими исходными данными. Студенту предлагается применить методику к новому набору исходных данных. Вопросы-задачи следуют стразу за вопросами примерами, имеют аналогичную или близкую формулировку, но пример решения уже не приводится. Во время тестирования студент при необходимости всегда может вернуться к вопросу-примеру.

Учебные тесты особенно важны при использовании на заочном обучении, где аудиторных часов очень мало, а центр тяжести в обучении переносится на самостоятельную работу.

Очень важную роль при организации тестирования играет правильная настройка параметров теста. Необходимо добиться такой ситуации, при которой студент должен подходить к тестированию подготовленным. Тест ни в коем случае не должен заменить собой чтение учебного материала. Анализ многих тестов, представленных в ЭОС, показывает, что часто преподаватели используют настройки, заданные по умолчанию при создании теста, видимо предполагая, что они самые оптимальные [2]. Хотя, во-первых, это не так, и, во-вторых, настройки должны быть разными для разных типов тестов и разных форм обучения. Вот некоторые негативные последствия определенных настроек теста.

При определенных параметрах теста студент сразу же после первой попытки может увидеть, как правильно отвечать на вопросы, и чтение учебников становится не нужным. При использовании адаптивного режима, студент может за одну попытку многократно вводить ответ и таким образом подбирать правильный, что, в общем, методически неверно. При использовании неограниченного количества попыток прохождения теста студент вместо чтения конспекта может «натаскивать себя» путем многократного прохождения теста и подбора правильных ответов таким образом. Надо заметить, что студенты никогда не скажут, что тесты настроены неправильно, потому что они думают, что так и надо. Но какое мнение сложится у студента о преподавателе, если тест настроен так, чтобы все могли на него ответить. Значит, идет борьба не за качество обучения, а за процент положительных оценок. А это, согласитесь, разные цели.

При настройке теста задаются следующие параметры (рис. 2 и 3):

– дата и время начала и окончания теста;

– ограничение времени ответа на вопросы;

– количество попыток;

– метод оценивания;

– порядок расположения вопросов в тесте;
– отображение вопросов на экране во время тестирования;
– случайный (или нет) порядок ответов в вопросах с выбором ответа;
– обучающий режим (да/нет);
– начислять штрафы (да/нет);
– настройки просмотра результатов теста студентом;
– пароль для доступа к тесту.

Другие настройки пока рассматривать не будем.

Каждый вид настройки в тесте должен быть обоснован.

Опыт использования тестов позволяет сформулировать следующие рекомендации.

Указание времени начала и окончания теста (1) оправдано в очень ограниченных ситуациях:

– на очном обучении, если курс используется для 1-й группы;

– для контрольных тестов – дата и время окончания теста указывается непосредственно перед прохождением теста; при этом начало можно не указывать.

Если тестом пользуются студенты нескольких групп, и особенно студенты всех форм заочного обучения, разные преподаватели, задавать начало и окончание тестирования не рекомендуется.

Говоря об ограничении времени прохождения теста (2), надо иметь в виду, что все виды промежуточного внутрикурсового тестирования так или иначе нацелены на итоговый тест, который всегда имеет ограничение по времени. Поэтому и все промежуточные тесты должны иметь ограничение по времени. Но эта общая рекомендация имеет свои разновидности. Так для студентов очного и заочного обучения длительность ограничения должны быть разной. Тест «Работа с учебником» должен иметь длительность, достаточную и для спокойного прочтения учебника, и для поиска ответа на вопросы. В этом случае возможно не стоит устанавливать ограничение по времени. Здесь также можно использовать адаптивный режим с возможностью нескольких попыток ответа на вопрос во время прохождения теста. Учебные тесты, моделирующие практическое занятие по решению задач, могут иметь ограничение равное длине реального практического занятия. В этих тестах можно и не задавать ограничение. В целом ограничение теста по времени организует студента, заставляет его подготовиться определенным образом к тесту, а также и анализировать свою подготовку и по временному фактору.

Количество попыток (3) надо ограничивать, что заставит студента «дорожить» попытками и не разбрасываться ими понапрасну. Очень интересна методика использования метода оценивания (4) «Средняя оценка» в сочетании с ограничением количества попыток. Студенту предлагается при самостоятельном тестировании обязательно пройти, например, 5 попыток, и при этом система будет выставлять среднюю оценку. Итоговая оценка, выставленная системой, нормируется на количество попыток, т.е. если студент прошел вместо 5-ти попыток только 3, то окончательная оценка за тест будет составлять 3/5 от итоговой. Такой подход «заставляет» студента использовать все попытки, что в свою очередь позволяет познакомиться с большим количеством вопросов из базы, а значит, качество обучения будет выше. Правда использование этой методики пока приходится проводить в полуавтоматическом режиме, т.к. система пока не позволяет сформировать отчет о количестве пройденных попыток студентами в группе, хотя настройку такого отчета можно было бы сделать системным администраторам.

Порядок вопросов в тесте (5) «как показано на экране редактирования» отображает тестовые вопросы в той последовательности, как их внес преподаватель в тест. Надо иметь в виду, что в этом случае в тест все вопросы включаются только при создании теста и далее он имеет статичную структуру, т.е. количество вопросов и порядок их следования не меняется при многократном прохождении теста. При дальнейшем расширении базы вопросов в тест с такими настройками невозможно будет добавить новые вопросы. Придется только создавать тест заново. Это недостатки такой настройки. Тем не менее, такую настройку рекомендуется использовать в тестах типа «Работа с учебником» и «Учебный тест», рассмотренных выше. Для других типов тестов порядок должен быть задан случайным. При случайной выборке вопросов из базы каждая новая попытка теста будет отличаться от предыдущей, что делает тест динамичным. При добавлении вопросов в базу они также будут включаться случайным образом в тест.

Рекомендуется также устанавливать отображение на экране вопросов (6) «по одному вопросу на каждой странице теста». Это позволяет студенту сосредоточиться на одном вопросе. Эта установка также важна при проведении итогового тестирования. Коснемся методики проведения итогового тестирования. Первая проблема заключается в том, какие вопросы и сколько включать в тест итогового контроля. Если база тестовых вопросов мала, то возможно надо включить все вопросы. А если база вопрос достаточно большая, то тест должен обеспечить проверку знаний по всем темам, вопросы для разных студентов должны быть одинакового уровня сложности, и тест должен иметь ограниченную длительность порядка 30-45 минут. Оптимальным здесь видится тест с одинаковыми вопросами для всех студентов. Так проводят тесты ЕГЭ и другие тесты централизованного массового тестирования. Тесты с одинаковыми вопросами повышают объективность оценки и позволяют преподавателю анализировать уровень сложности теста.

Отображение на экране только одного вопроса и случайный порядок их отображения в тесте не позволяет студенту сравнивать свои вопросы с теми, которые попались другому студенту. В таком тесте для обеспечения индивидуальной работы каждого тестируемого также можно установить настройку «последовательное прохождение теста», которая не позволит вернуться к предыдущим вопросам и изменить ответ.

О негативных сторонах обучающего режима (8) было сказано выше.

В режиме просмотра результатов теста ответы (10) во всех видах теста рекомендуется установить настройку отображения ответов студента («Свои ответы»), и не отображать правильные ответы теста («Ответы»), чтобы студент сам анализировал свои ошибки, а не получал ответы в готовом виде. При контрольном тестировании следует снять, в том числе, и флажок «Свои ответы», оставить только «Отзыв» и «Баллы».

Если вы проводите контрольное тестирование в присутствии преподавателя, то рекомендуется установить пароль доступа к тесту (11). Пароль вводит преподаватель перед началом тестирования. Если в компьютерном классе установлена программа подключения к столам студентов, например, NetOpSchool, то это можно сделать прямо с рабочего места преподавателя. Ввод пароля гарантирует, что тестирование проходит именно тот студент, который сейчас сидит в классе, а не кто-то удаленный за студента. При других вариантах доступа к тесту это в принципе возможно.

В заключении хочется дать общую рекомендацию администрации вузов. Использованием LMS-систем в учебном процессе и, в частности, применением тестирования, следует управлять, не пуская этот процесс на самотек, потому что от того, как построен процесс тестирования, во многом зависит и успешность обучения, и мнение студентов о конкретном преподавателе и о вузе вообще [3]. Рассмотренные в статье вопросы могут показаться очевидными опытному пользователю, владеющему компьютерными технологиями и хорошо знакомому с LMS Moodle. Однако, в целях дальнейшего повышения качества использования системы в учебном процессе необходимо обучать преподавателей некомпьютерных дисциплин педагогически и технологически правильному использованию возможностей тестирования с помощью курсов повышения квалификации, что в настоящий момент еще далеко от совершенства.

СПИСОК ЛИТЕРАТУРЫ

1. Титова Ю.Ф. Задачи и проблемы организации электронного обучения и применения дистанционных образовательных технологий // Академия профессионального образования. - 2015 - №6
2. Барабаш П.А., Воробьев С.П., Курносов В.И., Советов Б.Я. Инфокоммуникационные технологии в Глобальной информационной инфраструктуре – Санкт-Петербург. : Наука, 2008, 552 с.
3. Титова Ю.Ф. Об особенностях труда педагогических работников при использовании электронного обучения.// IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2017)» / Материалы конференциию - СПОИСУ. – СПб, 2016.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ

УДК 004.056

НАУЧНО-МЕТОДИЧЕСКИЕ ПОДХОДЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ТРАНСПОРТЕ

Белов Андрей Сергеевич[1], Барабанов Владимир Викторович[2]
[1]Михайловская военная артиллерийская академия, Россия, Санкт-Петербург, ул. Комсомола, 22
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14 линия, 39
e-mails: andrej2442016@yandex.ru,vlbar@yandex.ru

Аннотация. В статье рассматривается процесс ведения нарушителем несанкционированного мониторинга информационных систем посредством анализа демаскирующих признаков, а также предлагается способ управления демаскирующими признаками информационных систем на транспорте, как один из вариантов обеспечения их безопасности.

Ключевые слова: *демаскирующий признак, программное воздействие, информационные системы, способ управления.*

SCIENTIFIC AND METHODOLOGICAL APPROACHES TO ENSURE SAFETY OF INFORMATION SYSTEMS IN TRANSPORT

Belov Andrey[1], Barabanov Vladimir[2]
[1]Mikhailovskaya military artillery Academy
Russia, St. Petersburg, Komsomola str., 22
[2]St. Petersburg Institute of Informatics and Automation of the Russian Academy of Sciences
Russia, St. Petersburg, 14 line, 39
e-mails: andrej2442016 @ yandex.ru, vlbar @ yandex.ru

Abstract. The article deals with the process of keeping the infringer of unauthorized monitoring of information systems by means of analysis of unmasking features, and also provides a way to manage the unmasking features of information systems in transport as one of the options for ensuring their safety.

Keywords: *unmasking feature, software impact, information systems, management method.*

С развитием информационных и телекоммуникационных технологий, совершенствованием средств связи, обработки, хранения и распределения информации, становится актуальным процесс развития информационных систем (ИС), заключающийся в переходе к новым, более совершенным формам и организации сетей связи путем цифровизации и интеграции их в общемировое телекоммуникационное пространство.

В свою очередь, интеграция ИС на транспорте в общемировое телекоммуникационное пространство существенно увеличивает возможности нарушителей по их идентификации, вскрытию и воздействию [1-3].

Анализ информационных систем осуществляется нарушителем посредством ведения несанкционированного мониторинга (Рис. 1).

Из Рис. 1 видно, что процесс ведения несанкционированного мониторинга ИС осуществляется поэтапно. Сначала определяются цели мониторинга (необходимость определения состава ИС, вскрытие структуры, либо выявление алгоритмов функционирования ИС).

Далее анализируются (исследуются) демаскирующие признаки ИС и процессов их функционирования. Процесс анализа демаскирующих признаков реализуется двумя подсистемами: активной и пассивной. Пассивное исследование осуществляет сбор типовых демаскирующих признаков ИС. К типовым демаскирующим признакам относятся: форма огибающей сигнала; спектр сигналов; вид излучения, вид модулирующего сигнала; значения параметров сигнала; мощность излучения; количество излучаемых фиксированных частот и величины разноса между ними, взаимные удаления элементов по пеленгам (средств, комплексов, узлов связи); площадь размещения транспортных средств и др. [4-7].

Активное исследование предполагает использование деструктивных комплексных программных воздействий, включающих совокупность воздействий различных классов, объединенных единым сценарием.

В настоящее время наиболее часто реализуемые программными воздействиями являются [8-11]: анализ сетевого трафика, сканирование ИС, угроза выявления пароля, подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа, навязывание ложного маршрута ИС, внедрение ложного объекта ИС, отказ в обслуживании; удаленный запуск приложений.

Рис. 1- Обобщенный порядок проведения несанкционированного мониторинга ИС (вариант)

Множество характеристик описания процесса комплексных программных воздействий на ИС со стороны злоумышленника представляется в виде [12-15]:

$$U = \left\{ (u_1^{\text{ДПВ}},\ldots,\ u_n^{\text{ДПВ}}), (u_1^{\text{ПЗ}},\ldots,\ u_m^{\text{ПЗ}}), (u_1^{\text{НСД}},\ldots,\ u_k^{\text{НСД}}) \right\},$$

где $u_1^{\text{ДПВ}},\ldots,\ u_n^{\text{ДПВ}}, u_1^{\text{ПЗ}},\ldots,\ u_m^{\text{ПЗ}}, u_1^{\text{НСД}},\ldots,\ u_k^{\text{НСД}}$ - подмножества характеристик деструктивных программных воздействий, процесса преодоления системы защиты ИС и осуществления несанкционированного доступа (НСД) соответственно, n, m, k - число типов соответствующих воздействий.

В свою очередь каждое подмножество $u_i \in U$ имеет следующие характеристики: τ_i - оценка интервала времени между проведением каждого из воздействий *i*-го типа; T_i - оценка времени реализации воздействия *i*-го типа; V_i - оценка величины потенциального ущерба, нанесенного ИС в случае реализации воздействия*i*-го типа.

После анализа демаскирующих признаков переходят к формированию множества вариантов построения ИС, необходимых злоумышленнику для проведения полноценного исследования. Основными группами таких вариантов являются: варианты состава ИС, ее структуры и алгоритмов функционирования.

Формирование вариантов ИС включает в себя не только прямое отображение параметров по демаскирующим признакам, но также их обобщение и интеллектуальный анализ, что в конечном итоге позволит сформировать «типовые образы» ИС, отражающие ее функциональные особенности [16,17].

Таким образом, в настоящее время становится актуальным вопрос по разработке научно-методического обеспечения, практических рекомендаций, а также средств, методов (способов) и систем защиты, соответствующих современным условиям безопасного функционирования ИС и их элементов в условиях ведения злоумышленником несанкционированного мониторинга.

При решении вопросов разработки средств, методов и систем защиты ИС необходимо [4]:

– определить цели защиты;
– провести анализ демаскирующих признаков и возможных каналов утечки информации;
– оцеить возможности злоумышленника по осуществлению несанкционированных воздействий;
– разработать и осуществить технически и экономически обосновнные меры, способы и системы защиты;
– обеспечить контроль эффективности принимаемых мер защиты.

Анализ существующих средств и методов защиты позволил определить, что демаскирующие признаки ИС, выявляемые активным исследованием, могут быть скрыты методами разграничения доступа (в частности межсетевого экранирования) и криптографического закрытия семантической составляющей информационного обмена [18,19].

Однако существующие методы защиты не всегда эффективны. В связи с этим возникает необходимость разработки научно-методических подходов, позволяющих осуществлять формирование защищенных ИС, путем управления (ослабления, устранения) их демаскирующими признаками.

В качестве научно-методического подхода разработан способ управления демаскирующими признаками ИС, основанный на варьировании значениями управляемых демаскирующих признаков по соответствующим правилам и в заданных пределах, в результате чего, злоумышленник вводится в заблуждение относительно структуры ИС и параметров их функционирования, что приводит к повышению устойчивости ИС в условиях деструктивных программных воздействий [19,20].

Обобщенная схема, поясняющая способ управления демаскирующими признаками ИС представлена на рис. 2.

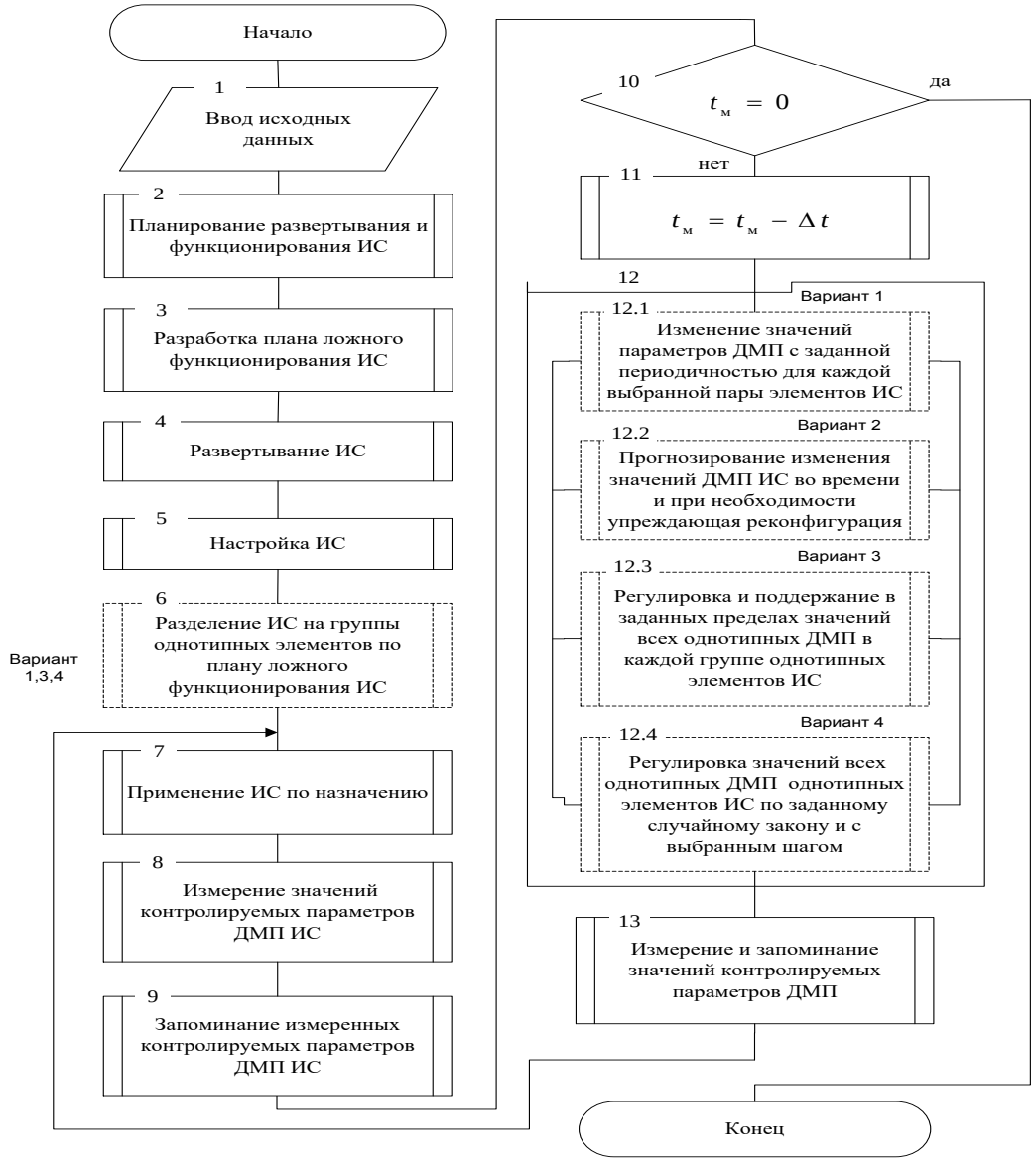


Рис. 2- Обобщенная схема способа (вариантов) управления демаскирующими признаками ИС

В качестве исходных данных задают множество контролируемых параметров демаскирующих признаков ИС, представляемое в виде:

$$N = \left\{ N_1 , N_2 ,..., N_{n-1},..., N_{\text{n}} \right\},$$

где N – множество контролируемых параметров демаскирующих признаков ИС, причем $N \geq 2$.

В результате измерения значений данных контролируемых параметров, в ходе выполнения цикла анализа, формируют $G \geq 2$ групп контролируемых параметров демаскирующих признаков и задают коэффициенты важности – (k_1,k_2…k_n) для каждой G-ой группы:

$$G = \left\{ k_1(N_{G_1}), k_2(N_{G_2}),..., k_{n-1}(N_{G_{n-1}}),..., k_n(N_{G_n}) \right\}.$$

Дополнительно определяется количество управляемых и неуправляемых демаскирующих признаков. Перед развертыванием, разрабатываются варианты ложного функционирования ИС. После этого осуществляют развертывание ИС, настраивают основные параметры и применяют ее по назначению. На функционирующей ИС производят измерение значений контролируемых параметров демаскирующих признаков и запоминают их с целью дальнейшего использования.

Способ предполагает управление защищенностью ИС путем нескольких научно-методических подходов (вариантов обеспечения безопасности ИС).

В первом варианте злоумышленник вводится в заблуждение относительно структуры ИС и их параметров за счет периодического (по необходимости корректируемого) взаимного изменения демаскирующих признаков на выбранных парах элементов ИС.

Во втором варианте злоумышленник вводится в заблуждение относительно структуры ИС и их параметров на основе прогнозирования значений показателей демаскирующих признаков и, при необходимости, упреждающей реконфигурации ИС.

В третьем варианте злоумышленник вводится в заблуждение относительно структуры ИС и ее параметров за счет принудительной регулировки (с заданной периодичностью) и поддержания в установленных пределах на однотипных элементах ИС значений всех однотипных признаков.

В четвертом варианте злоумышленник вводится в заблуждение относительно структуры ИС и ее параметров за счет одновременного изменения всех однотипных параметров демаскирующих признаков в каждой группе всех однотипных элементов ИС по заданному случайному закону и шагу с заданным периодом так, чтобы параметры демаскирующих признаков элементов ИС попали в заданный интервал значений.

Таким образом, в каждом варианте, на основе измерения и прогнозирования характеристик демаскирующих признаков ИС, реализована возможность корректировки (изменения и поддержания) значений управляемых демаскирующих признаков их элементов в заданных значениях и упреждающей реконфигурации. Это, в конечном итоге, снижает эффективность несанкционированного мониторинга и преднамеренных деструктивных программных воздействий.

Научно-методические подходы реализованы в виде патента РФ на изобретение [20]. Кроме того, полученные результаты могут использоваться при проведении исследований и выполнении научно-исследовательских работ по разработке методов и способов защиты ИС в условиях внешних деструктивных программных воздействий, а также при проектировании систем защиты ИС в рамках определения защитного ресурса.

СПИСОК ЛИТЕРАТУРЫ

1. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. СПб.: БХВ - Петербург, 2003. – 368 с: ил.
2. Теоретические основы создания систем поддержки принятия решений в интересах комплексной транспортной безопасности/ А.М. Сазыкин [и др.]// Известия Российской академии ракетных и артиллерийских наук. 2015. № 3. С. 10-15.
3. Проблема сравнения и выбора варианта построения системы безопасности/ В.В. Барабанов [и др.]/ В сборнике: Актуальные проблемы защиты и безопасности. - Труды Четвертой Всероссийской научно-практической конференции. 2001. С. 348-351.
4. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки. – М.: Российск. гос. гуманит. ун-т, 2002. – 399 с.
5. Показатели эффективности межведомственного информационного взаимодействия при управлении обороной государства/ Е.Г. Анисимов, В.Г. Анисимов [и др.]// Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. № 7-8 (97-98). С. 12-16.
6. Анисимов В.Г., Селиванов А.А., Анисимов Е.Г. Методика оценки эффективности защиты информации в системе межведомственного информационного взаимодействия при управлении обороной государства// Информация и космос. 2016. № 4. С. 76-80.
7. Риск-ориентированный подход к организации контроля в подсистемах обеспечения безопасности информационных систем/ П.Д. Зегжда [и др.]// Проблемы информационной безопасности. Компьютерные системы. 2016. № 3. С. 61-67.
8. Руководящий документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). – М.: ФСТЭК, 2008. – 69 с.
9. Модели организации и проведения испытаний элементов системы информационного обеспечения применения высокоточных средств/ В.В. Барабанов [и др.]// Труды Военно-космической академии им. А.Ф. Можайского. 2015. № 648. С. 6-12.
10. Модель оценки эффективности информационного обеспечения применения высокоточного оружия в контртеррористических операциях/ А.Ю.Гарькушев, А.М. Сазыкин[и др.]// Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2015. № 1-2. С. 44-53.
11. Методика расчета латентного эффекта применения системы управления рисками/ В.Г. Анисимов Е.Г., Анисимов [и др.]// Вестник Российской таможенной академии. 2015. № 2 (31). С. 115-123.

12. Алгулиев Р. М.Угрозы корпоративным сетям и формализация их отношений с системами защиты. – Баку, 2000. – 30 с.
13. Основы построения моделей интеллектуализации в системах безопасности/ А.Ю.Гарькушев, А.М. Сазыкин [и др.]// Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2014. № 9-10. С. 22-27.
14. Модель причинного анализа на основе использования данных об особых ситуациях/ *В.В. Балясников, Ю.В. Ведерников* [и др.]// Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2015. № 1-2. С. 31-38.
15. Расчет эффективности межведомственного информационного взаимодействия в области обороны государства/ Е.Г. Анисимов [и др.]/ В сборнике: Система межведомственного информационного взаимодействия при решении задач в области обороны Российской Федерации. Сборник материалов II Межведомственной научно-практической конференции. Национальный центр управления обороной Российской Федерации/ Под общей редакцией И.В. Солохова.- 2016. С. 21-26.
16. Показатели эффективности защиты информации в системе информационного взаимодействия при управлении сложными распределенными организационными объектами/ Т.Н. Сауренко, С.П. Присяжнюк [и др.]// Проблемы информационной безопасности. Компьютерные системы. 2016. № 4. С. 140-145.
17. Петренко С. А. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия. – Труды ИСА РАН, том 41, 2009. 104-146 с.
18. Белов А. С. и др. Способ защиты автоматизированных систем. Патент РФ на изобретение № 2408927 от 21 июля 2009 г. – 11 с.
19. Белов А. С. и др. Способ контроля демаскирующих признаков системы связи. Патент РФ на изобретение № 2419153 от 30 июня 2009 г. – 22 с.
20. Белов А. С. и др. Способ (варианты) управления демаскирующими признаками системы связи. Патент РФ на изобретение № 2450337 от 10 мая 2012 г. – 19 с.

УДК 004.056

ТОР-10 УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ VANET: АНАЛИТИЧЕСКИЙ ОБЗОР[3]

Буйневич Михаил Викторович, Столярова Екатерина Сергеевна, Хорошенко Сергей Викторович,
Ширяев Денис Михайлович, Владыко Андрей Геннадьевич
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
Россия, Санкт-Петербург, пр. Большевиков, 22, корп. 1
e-mails: bmv1958@yandex.ru, ekaterinastoljarova@rambler.ru, khoroshenko@sut.ru,
shiryaev.dm@spbgut.ru, vladyko@sut.ru

Аннотация. В статье представлен аналитический обзор публикаций, посвященных вопросам безопасности функционирования автомобильных беспроводных сетей (VANET), как инфокоммуникационных систем. Наиболее «популярные» угрозы анализируются по схеме: атака – уязвимость – ущерб – контрмеры. Показываются направления дальнейших исследований проблемных вопросов противодействия угрозам информационной безопасности VANET.

Ключевые слова: *VANET; информационная безопасность; угроза; обзор.*

THE TOP-10 INFORMATION SECURITY THREATS IN VANET: ANALYTICALSURVEY

Mikhail Buinevich, Ekaterina Stolyarova, Sergei Khoroshenko, Denis Shiryaev, Andrei Vladyko
Bonch-Bruevich St. Petersburg State University of Telecommunications,
Russia, St. Petersburg, Bolshevikspr., 22/1
e-mails: bmv1958@yandex.ru, ekaterinastoljarova@rambler.ru, khoroshenko@sut.ru,
shiryaev.dm@spbgut.ru, vladyko@sut.ru

Abstract. The analytical survey of foreign publications about safety of functioning of vehicular ad hoc networks (VANET), as infocommunication systems, is presented. The most "popular" threats are analyzed according to the scheme: attack – vulnerability– damage – countermeasures. The directions of the further researches of problematic issues of counteraction to information security threats in VANET are shown.

Keywords: *VANET; information security; threat; survey.*

Введение. Сети VANET (от англ. vehicular ad hoc network – автомобильные беспроводные сети) – это передовые инфокоммуникационные технологии, нацеленные на обеспечение повышения безопасности и эффективности дорожного движения за счет обмена информацией между транспортными средствами (OBU, от англ. board unit) и объектами дорожной инфраструктуры (RSU, от англ. road-side unit). OBU могут работать в режиме V2V (от англ. vehicular to vehicular), V2I (от англ. vehicular to infrastructure) или в гибридном режиме, что позволяет за одну или несколько итераций обмениваться сообщениями со всеми участниками сети. Это обеспечивает информирование и предупреждение водителей транспортных средств о возможных препятствиях (ремонтных работах, ограничении скорости etc), а также возможность организации согласованных действий (смена полос, приоритетный проезд перекрестков etc). Поэтому любое нарушение функционирования VANET автоматически влияет на безопасность людей и техники на дороге, что возводит вопросы угроз ее информационной безопасности в ранг «сверхактуальных», о чем свидетельствует нарастающий вал

[3] Исследование выполнено при финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (Соглашение № 14.604.21.0165, уникальный идентификатор проекта RFMEFI60417X0165).

зарубежных публикаций на эту тему. Отсутствие успешных реализаций концепции VANET в России и, как следствие, так называемых BestPractice, сопровождается слабой публикационной активностью и явно недостаточной информированностью широкого круга отечественных специалистов по этому разделу информационной безопасности.

С точки зрения ущерба от реализации угроз информационной безопасности, все атаки на VANET можно условно идентифицировать по признакам нарушения (компрометации) того или иного свойства ее информационных ресурсов – конфиденциальности, целостности и доступности – или их комбинации.Доступность гарантирует, что сеть функционирует и отражает необходимую информацию в любое время; это является критическим требованием безопасности VANET, так как в противном случае нет возможности реализовать ее главный функционал –информирование и предупреждение.Конфиденциальность гарантирует, что эта информация используются только авторизованными узлами, а целостность – что она не изменялась никем, кроме как ими (авторизованными узлами).

Проведенный авторами анализ многочисленных источников, описывающих проблематику информационной безопасности в сетях VANET, позволил составить перечень из наиболее «популярных» угроз, представленный в таблице 1.

Таблица 1

Перечень «популярных» угроз информационной безопасности в автомобильных беспроводных сетях

Угроза (атака)	Нарушение информационной безопасности	Источник
DoS	Доступность	[1, 2], [12], [14], [14], [24], [25],[26]
Tracking	Конфиденциальность	[2], [3], [8], [14], [15], [16], [17], [18],[19], [21], [22], [29], [30]
Routing: Blackhole, Greyhole, Wormhole, Tunnelling	Целостность	[2], [4], [7], [38]
Tampering Hardware	Конфиденциальность, целостность, доступность	[5]
Sybil attack	Доступность, целостность	[3], [6], [7], [27], [28], [29], [30], [31], [32], [33], [34]
Traffic analysis	Конфиденциальность	[2], [8], [9], [10], [13], [22], [46]
Jamming	Доступность	[11], [25]
GPS-spoofing / Position faking	Конфиденциальность, целостность	[7], [12], [15], [35]
Timingattack	Конфиденциальность	[7], [14], [26]
Message tampering/ suppression / fabrication	Конфиденциальность, целостность	[1], [13], [15], [16], [23], [35], [33], [34], [37], [40], [41], [42]
Man in the middle	Конфиденциальность, целостность	[7], [26], [35], [36], [37]
Brute force	Конфиденциальность	[29], [38], [39]
Broadcas t tampering	Доступность	[5]
Node impersonation	Конфиденциальность, целостность	[2], [15], [19], [27], [29], [31], [37]
Replay	Конфиденциальность	[2], [15], [33]
Illusion attack	Целостность	[12] ,[15], [35]
Key and / or certificate replication (unauthorized access)	Конфиденциальность, целостность	[3], [14], [20], [23], [28], [29]
Malware Spamming	Конфиденциальность, доступность	[31]
Loss of event traceability	Доступность, целостность	[7], [23], [31]

Такое изобилие угроз предполагает их систематизацию и структуризацию; авторами в докладе «Классификационные признаки угроз информационной безопасности VANET» на ИБРР-2017 проведен критический анализ подходов к классификации, представленных в соответствующих обзорах ([21, 43]).

Проанализируем условную «первую десятку» (Top-10 по количеству ссылок) угроз из представленного списка. Анализ проведем по классической схеме: атака – эксплуатируемая уязвимость – ущерб информационной безопасности – контрмеры.

1) *Sybi*l – разрушение репутации сети путем клонирования ложных идентификаторов. Эксплуатируя уязвимость простой множественной подделки идентификатора, злоумышленник создает клоны идентификационных данных для получения непропорционально большого влияния на сеть, многократно имитируя функционирование валидных узлов. Атака наносит прямой ущерб доступности сети, засоряя трафик ложными сообщениями, а также увеличивает вероятность отправки данных через узел злоумышленника (см. ниже атаку «Man in the middle»), что потенциально ведет к нарушению конфиденциальности, так как злоумышленник прочитает трафик, ему

непредназначенный. С помощью данной атаки злоумышленник может влиять и на целостность, например, отправлять ложные сообщения дорожной обстановке. Меры предотвращения: созданием доверительного канала (например, за счет валидации идентификационных данных).

2) *Node impersonation* – подмена идентификации участника дорожного движения. Атака реализуется путем подмены злоумышленником своих MAC- и IP- адресов на адреса валидного узла. Для получения идентификационных данных других узлов злоумышленник использует соответствующий спуфинг. При отсутствии аутентификации атакующий может отправить ложное сообщение от имени другого узла, тем самым нарушая целостность. Например, машина представляется автомобилем скорой помощи для получения права приоритетного проезда. При обратной операции, т.е. получении сообщения, предназначенного автомобилю с искомыми IP- и MAC-адресами, будет нарушена конфиденциальность. Меры предотвращения: аутентификация, основанная на сертификатах, динамические адреса.

3) *Man in the middle*– перехват и модификация сообщений между автомобилями и точками доступа. Данную атаку можно реализовать в двух вариациях: для режима OBU и для режима RSU. В первом случае узел злоумышленника (OBU) «слушает» канал соединения между другими узлами. В случае с RSU злоумышленник организует точку доступа (передатчик) на участке дороги для перехвата (нарушение конфиденциальности) и модификации (нарушение целостности) сообщений; передатчик атакующего при этом подключается к основному передатчику. Другие узлы подключаются к лже-передатчику и передают сообщения через него на основной передатчик, при этом злоумышленник получает всю информацию, идущую на основной передатчик от абонентов, так как являлся несанкционированным посредником между ними. Меры предотвращения: цифровые сертификаты в совокупности с методами аутентификации, а также хэширование с ключами.

4) *GPS-spoofing / Hidden vehicle (position faking)*– подмена координат местоположения узла. Используя GPS-симулятор, злоумышленник генерирует сигнал, превосходящий мощностью реальный сигнал спутника. Транспортные средства считывают более сильный, ложный сигнал, который транслирует автомобилю неверное местоположение, принимаемое за истинное. Атака «Hidden vehicle» является частным случаем подмены данных о местоположении, когда узел умышленно не посылаются предупреждающие сообщения другому узлу о месте ДТП. Такого рода атаки направлены на нарушение целостности сообщений, отправляемых узлом со своим местоположением, так как в процессе атаки эти данные модифицируются злоумышленником. Меры предотвращения: может быть рекомендована цифровая подпись данных о местоположении (данный вопрос дискутируется в научном сообществе, т.к. метод абсолютного устранения данной угрозы еще не выявлен).

5) *Traffic analysis*– определение топологии сети, маршрутизации. Атака заключается в перехвате и анализе различного рода служебных и информационных пакетов, которые могут содержать в себе местоположение, идентификационные данные, маршрут и т.д. Такой вид пассивной атаки позволяет злоумышленнику подготовиться к реализации мощной активной атаки. Анализ трафика нарушает конфиденциальность передачи сообщения для всех режимов обмена OBU и RSU. Меры предотвращения: создание защищенного канала передачи информации.

6) *Key and / or certificate replication* – неавторизованная идентификация в системе. Атака представляет собой использование дубликатов ключей, сертификатов или их комбинации для неавторизованной идентификации пользователя в системе. Злоумышленник подрывает работу системы, дублируя идентификационные данные других узлов. Его цель состоит в том, чтобы перепутать полномочия и предотвратить идентификацию участников ДТП. Данная атака наносит прямой ущерб конфиденциальности данных, а также от нее страдает целостность, т.к. при реализации атаки злоумышленник может перераспределить роли участников в ДТП в свою пользу. Меры предотвращения: создание защищенного канала передачи информации; имеет место для обсуждения использование ключей с ограниченным сроком действия, во избежание использования ключа злоумышленником.

7) *DoS (Denial of Service)* – отказвобслуживании. Наиболее известная атака для большинства сетей, цель которой в данном классе – довести VANET до отказа или увеличить задержки в сети, что сделает невозможным или затруднит получение информации легитимными пользователями. Поскольку информация в автомобильных беспроводных сетях очень быстро устаревает, то даже небольшие задержки могут свести работу отдельного сегмента к нулю, так как в момент получения информации дорожная ситуация уже будет совершенно иной. Данная атака наносит прямой ущерб доступности сети и имеет много вариаций. Многие исследователи относят в ней все атаки на маршрутизацию и/или потребление ресурсов. На данный момент существует много методов противодействия DoS-атакам, однако их эффективность до сих пор под вопросом.

8) *Routing: blackhole, greyhole, wormhole, tunneling etc.* – несанкционированый доступ к конфиденциальной информации, нарушение маршрута следования данных. Атака эксплуатирует уязвимость протоколов маршрутизации сетевого уровня и имеет несколько разновидностей. Blackhole («черная дыра») направлена на уничтожение всех пакетов, которые следуют через узел злоумышленника; следовательно, пакеты не приходят к получателю. Greyhole («серая дыра») направлена на уничтожение только некоторой части пакетов, т. к. это уменьшает вероятность, что

злоумышленник будет обнаружен соседними узлами; остальные пакеты транслируются правильно. Очевидно, что все эти атаки направлены на нарушение целостности передаваемых данных. Меры предотвращения: в реферируемых источниках не найдены.

9) *Tracking*– несанкционированный доступ к идентификационной информации об узле. Данная атак направлена на отслеживание местоположения транспортного средства в течение промежутка времени для получения детальной информации об узле. Направлена на нарушение конфиденциальности данных легитимного узла, т. к. злоумышленник стремится перехватить их и использовать в своих целях. Меры предотвращения: в реферируемых источниках не найдены.

10) *Messagetampering / suppression / fabrication*– атакинапередаваемыесообщения. Атака Message tampering направлена на нарушение целостности передаваемых сообщений: злоумышленник модифицирует сообщения OBU-OBU и OBU- RSU, при этом фальсификации могут быть подвержены, как запрос приложения, так и ответ на запрос. Атака Message Suppression направлена на нарушение конфиденциальности передаваемых сообщений: злоумышленник осуществляет выборку пакетов и транслирует их в сеть, доступ к которой имеют посторонние пользователи, не участвующие в валидном обмене этих пакетов; пакеты, в частности, могут содержать информацию, относящуюся к безопасности узла. Атака Message Fabrication направлена на нарушение целостности и конфиденциальности передаваемых сообщений: злоумышленник транслирует в сеть ложные сообщения; подобным образом злоумышленник может получить право приоритетного проезда, неавторизованный доступ к системным ресурсам и конфиденциальным данным (пароли, логины других узлов). Меры предотвращения: в реферируемых источниках не найдены; можно предположить шифрование передаваемых пакетов и выдачу цифровых сертификатов для проверки подлинности узла.

Заключение.

Несмотря на обилие угроз, представленных в анализируемых источниках, практически все они характерны для любой беспроводной сети; к специфическим же угрозам именно для VANET можно отнести, пожалуй, только GPS-spoofing / Position faking [7].

Также не для всех угроз указаны эксплуатируемые злоумышленниками уязвимости, которые являются важнейшим фактором генерации требований к защитным мерам; последние также не указаны для отельных угроз.

Эти обстоятельства являются критическими для дальнейшего продвижения концепции VANET, поскольку в случае обнаружения высокоуровневых уязвимостей может потребоваться ревизия ее архитектурной модели. Поэтом актуальными следует признать исследования феномена VANET, как такой инфокоммуникационной системы, которая как наследует далеко не все уязвимости ее составных частей (например, беспроводной сети), так и приобретает принципиально новые.

СПИСОКЛИТЕРАТУРЫ

1. Karagiannis G., Altintas O., Ekici E., Heijenk G., Jarupan B., Lin K., Weil T. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions // IEEE Communications Surveys and Tutorials, 2011, vol. 13, iss. 4, pp. 584-616.
2. Raw R.S., Kumar M., Singh N. Security Challenges, Issues and Their Solutions for VANET // International Journal of Network Security and Its Applications, 2013, vol.5, no.5, pp. 95-105.
3. Samara G., Al-Salihy W.A.H., Sures R. Security Analysis of Vehicular Ad Hoc Networks (VANET) // Proceedings of the Second International Conference on Network Applications Protocols and Services (NETAPPS), Kedah, Malaysia, 2010, pp. 55-60.
4. Rawat A., Sharma S., Sushil R. VANET: Security Attacks and Its SpossibleSolutions // Journal of Information and Operations Management, 2012, vol. 3, iss. 1, pp. 301–304.
5. Hasrouny H., Samhat A.E., Bassil C., Laouiti A. VANet Security Challenges and Solutions: A Survey // Vehicular Communications, 2017, vol. 7, pp. 7-20.
6. van der Heijden R. Security Architectures in V2V and V2I Communication // Proceedings of the 13th Twenty Student Conference on IT, Enschede, The Netherlands, 2010.
7. Vinh H.L., Cavalli A.R. Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey", International Journal on AdHoc Networking Systems, 2014, vol. 4, no. 2, pp.1-20.
8. Whyte W., Weimerskirch A., Kumar V., Hehn T. A Security Credential Management System for V2V Communications // Proceedings of the IEEE Vehicular NetworkingConference (VNC), Boston, MA, USA, 2013, pp. 1-8.
9. Plößl K., Federrath H. A privacy aware and efficient security infrastructure for vehicular ad hoc networks // Computer Standards and Interfaces, 2008, vol. 30, iss. 6, pp. 390-397.
10. Abuelela M., Olariu S., Ibrahim K. A Secure and Privacy Aware Data Dissemination for the Notification of Traffic Incidents // Proceedings of the IEEE 69th Vehicular Technology Conference (VTC Spring 2009), Barcelona, Spain, 2009, pp. 1-5.
11. Malla A.M., Sahu R.K. Security attacks with an effective solution for Dos attacks in VANET // International Journal of Computer Applications, 2013, vol. 66, iss. 22, p. 45-49.
12. He L., Zhu W.T. Mitigating DoS Attacks Against Signature-Based Authentication in VANETs // Proceedings of the IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China, 2012, vol. 3, pp. 261–265.
13. Raya M., Aziz A., Hubaux J.P. Efficient Secure Aggregation in VANETs // Proceedings of the 3rd international workshop on Vehicular ad hoc networks (VANET '06), Los Angeles, CA, USA, 2006, pp. 67-75.
9. Raya M., Hubaux J.P. The Security of Vehicular Ad Hoc Networks", Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN'05), Alexandria, VA, USA, 2005, pp. 11-21.
10. ETSI TR 102 893 V1.1.1 (2010-03) Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA). ETSI, 2010.
11. Guo J., Baugh J.P., Wang S. A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework // Proceedings of the Mobile Networking for Vehicular Environments (MOVE), Anchorage, AK, USA, 2007, pp. 103-108.
12. Salem F.M., Ibrahim M.H., Ibrahim I.I. Non-Interactive Authentication Scheme Providing Privacy among Drivers in Vehicle-to-Vehicle Networks // Proceedings of the Sixth International Conference on Networking and Services (ICNS), Cancun, Mexico, 2010, pp. 156-161.

13. ETSI TS 102 941 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; Trust and Privacy Management. ETSI, 2012.
14. Engoulou R.G., Bellaïche M., Pierre S., Quintero A. VANET Security Surveys // Computer Communications, 2014, vol. 44 pp. 1-13.
15. Aslam B., Zou C.C. Distributed Certificate Architecture for VANETs // Proceedings of the IEEE Military Communications Conference (MILCOM), Boston, MA, USA, 2009. pp. 1-7.
16. Nema M., Stalin S., Lokhande V. Analysis of Attacks and Challenges in VANET // International Journal of Emerging Technology and Advanced Engineering, 2014, vol. 4, iss. 7, pp. 831-835.
17. Calandriello G., Papadimitratos P., Hubaux J.P., Lioy A. Efficient and Robust Pseudonymous Authentication in VANET // Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks (VANET '07), Montreal, Quebec, Canada, 2007, pp. 19-28.
18. Dahiya A., Sharma V. A Survey on Securing User Authentication Vehicular Ad Hoc Networks // International Journal of Information Security, 2001, vol. 1, 164–171.
19. Hasrouny H., Bassil C., Samhat A., Laouiti A. Security Risk Analysis of a Trust model for Secure Group Leader-based communication in VANET // Advances in Intelligent Systems and Computing, 2017, vol. 548, pp. 71-83.
20. Engoulou R. Securisation des vanets par reputation des nœuds. Thesis report. Ecole Polytechnique de Montreal, 2013.
21. Chuang M.C., Lee J.F. TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks // IEEE Systems Journal, 2013, vol. 8, iss. 3, pp. 749-758.
22. Al-Kahtani M.S. Survey on Security Attacks in Vehicular Ad Hoc Networks (VANETs) // Proceedings of the 6th International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, QLD, Australia, 2012, pp. 1–9.
23. Rao A., Sangwan A., Kherani A.A., Varghese A., Bellur B., Shorey R. Secure V2V Communication with Certificate Revocations // Proceedings of the Mobile Networking for Vehicular Environments, Anchorage, AK, USA, 2007, pp. 127-132.
24. Raya M., Papadimitratos P., Hubaux J.P. Securing Vehicular Communications // IEEE Wireless Communications, 2006, vol. 13, iss. 5, pp. 8-15.
25. Xiao B., Yu B., Gao C. Detection and localization of sybil nodes in VANETs // Proceedings of the workshop on Dependability issues in wireless ad hoc networks and sensor networks (DIWANS '06), Los Angeles, CA, USA, 2006, pp. 1–8.
26. Singelee D., Preneel B. Location verification using secure distance bounding protocols // Proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, Washington, DC, USA, 2005., 2005, p. 7.
27. Zhou T., Choudhury R.R., Ning P., Chakrabarty K. P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks //IEEE Journal on Selected Areas in Communications, 2011, vol. 29, no. 3, pp. 582-594.
28. Yan G., Olaruis S., Weigle M. Use of infrastructure in VANETs // Computer Communications, 2008, vol. 31, iss. 12, pp. 2883-2897.
29. Kushwaha D., Shukla P.K., Baraskar R. A survey on Sybil Attack in Vehicular Ad-hoc Network // International Journal of Computer Applications, 2014, vol. 98, no.15, pp. 31-36.
30. Song L., Han Q., Liu J. Investigate Key Management and Authentication Models in VANETs // Proceedings of the IEEE International Conference on Electronics, Communications and Control (ICECC), Ningbo, China, 2011, pp. 1516-1519.
31. Jung C.D., Sur C., Park Y., Rhee K.H. A Robust Conditional Privacy-Preserving Authentication Protocol in VANET // Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2009, vol. 17, pp. 35-45.
32. Raiya R., Gandhi S. Survey of Various Security Techniques in VANET // International Journal of Advanced Research in computer Science and Software Engineering, 2014, vol. 4, iss. 6, pp. 431-433.
33. Patel N., Jhaveri R.H. Trust based approaches for secure routing in VANET: A Survey // Procedia Computer Science, 2015, vol. 45, 2015, pp. 592-601.
34. Zeadally S., Hunt R., Chen Y.S., Irwin A., Hassan A. Vehicular Ad Hoc Networks (VANETs): Status, Results, and Challenges // Telecommunication Systems, 2012, vol. 50, iss. 4, pp. 217–241.
35. Caballero-Gil P. Security Issues in Vehicular Ad Hoc Networks / Mobile Ad-Hoc Networks: Applications. InTech, 2011, pp. 67-88.
36. Jayalakshmi N., Rajadurai R., Indumathi K. Vehicular Network: Properties, Structure, Challenges, Attacks, Solution for Improving Scalability and Security // International Journal of Scientific and Engineering Research, 2013, vol. 4, iss. 6, pp. 152-159.
37. Blum J., Eskandarian A. The Threat of Intelligent Collisions // IT Professional, 2004, vol. 6, iss. 1, pp. 24–29.
38. Sumra I.A., Ahmad I., Hasbullah H., Manan J. Classes of attacks in VANET // Proceedings of the Saudi International Electronics, Communications and Photonics Conference (SIECPC), Riyadh, Saudi Arabia, 2011, pp. 1-5.
39. Sumra I.A., Hasbullah H.B., Manan J, Ahmad I., Alghazzawi D.M. Classification of Attacks in Vehicular Ad hoc Network (VANET) // Information, 2013, vol. 16, no. 5, pp. 2995-3004.
40. Nema M., Stalin S., Lokhande V. Analysis of Attacks and Challenges in VANET // International Journal of Emerging Technology and Advanced Engineering, 2014, vol. 4, iss. 7, pp. 831-835.
41. Mousumi P., Gautam S. Traffic Analysis of Vehicular Ad-Hoc Networks of V2I Communication // Procedia Computer Science, 2015, vol. 54, pp. 215 – 223.
42. Mostovich D., Fabrikantov P., Vladyko A., Buinevich M. High-Level Vulnerabilities of Software-Defined Networking in the Context of Telecommunication Network Evolution // Proceedings of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg, Russia, 2017. pp. 184-186.
43. Buinevich M., Fabrikantov P., Stolyarova E., Izrailov K., Vladyko A. Software Defined Internet of Things: Cyber Antifragility and Vulnerability Forecast // Proceedings of the IEEE 11th International Conference on Application of Information and Communication Technologies (AICT), Moscow, Russia, 2017, pp. 293-297.

УДК 004.05

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДВИЖЕНИЯ СУДОВ

Бухарметов Максим Радикович, Нырков Анатолий Павлович
Государственный университет морского и речного флота
имени адмирала С.О.Макарова «ГУМРФ»,
Россия, Санкт-Петербург, ул. Двинская, 5/7
e-mails: kaf.koib@gmail.com, evrolittle@yandex.ru

Аннотация. В докладе рассмотрены задачи автоматизированного управления движением судов и вопросы информационного обеспечения автоматизированных систембезопасности движения судовна водных путях.

Ключевые слова: *водный транспорт; автоматизированные системы; безопасность.*

INFORMATION SECURITY OF TRAFFIC OF SHIPS

Bukharmetov Maxim, Nyrkov Anatoli
Admiral Makarov State University of Maritime and Inland Shipping,
Russia, St. Petersburg, Dvinskaya str., 5/7
e-mails: kaf.koib@gmail.com, evrolittle@yandex.ru

Abstract. In the report problems of automated management of the movement of vessels and questions of information support of the automated security systems of the movement of vessels on waterways are considered.

Keywords: *the water transport; the automated systems; safety.*

Автоматизированные системы управления движением судов (АСУДС), использующие устаревшие виды связей, не соответствуют требованиям международных стандартов обеспечения безопасности судоходства [1]. Для достижения цели объединения в единое коммуникационное пространство современных информационных систем различного вида транспорта необходимо повысить качество связи, что позволит в перспективе обеспечивать их оптимальную безопасность.

Автоматизированные системы управления движением судов играют немаловажную роль для обеспечения безопасности на водных путях [2-8]. Но в стремительно изменяющихся условиях одна из проблем отражает поиск путей управления движением судов на основе решений в области широкого информационного взаимодействия. Первостепенной задачей данного взаимодействия стоит модернизированное информационное обслуживание. Под модернизированным информационным обслуживанием здесь понимается переход к более высокому уровню, повышение качества и оперативности взаимообмена необходимой информацией между участниками водного транспортного процесса. С целью повышения безопасности судоходства новые системы информационного обслуживания должны обеспечивать объединение поступающей информации от различных внешних и внутренних систем, что позволит в реальном времени давать полное представление об обстановке в зоне действия. Также система должна осуществлять интеллектуальную обработку разнородных данных, приходящих от участников водного процесса, и в ответ формировать им исходящие информационные потоки с учетом необходимости и их запросов.

Такое построение системы взаимодействия наилучшим образом отвечает потребностям повышения безопасности судоходства. Для решения подобных задач необходимо создать профессиональную, целостную, комплексную систему, способную обеспечить гарантированную и надежную передачу навигационных данных в центры оперативного управления и диспетчерские пункты, которые проводят мониторинг и осуществляют контроль на водном внутреннем транспорте.

В критических инфраструктурах, к числу которых относится и водный транспорт, необходимо активно развивать и внедрять группу средств «превентивной» защиты информации, которые, позволяют принимать меры задолго до реальных угроз безопасности. К числу таких систем относятся системы мониторинга и управления безопасностью нового поколения. Данные системы обладают широкими интеллектуальными возможностями в области представления, хранения, обработки и отображения информации о безопасности. Высокая масштабируемость позволяет быстро увеличивать мощность системы, в соответствии с растущими требованиями. Кроме того, данные системы, предоставляют возможность обнаружения «редких» атак и совместного анализа событий безопасности на различных уровнях (сетевом уровне, уровне физических управляющих элементов/датчиков и бизнес–уровне) [9].

Автоматизированные системы управления движением судов и управляющие системы водного транспорта имеют достаточно многочисленное число систем, обрабатывающих большое количество разнородной информации. Учитывая весь спектр возможных угроз безопасности и критичность возможных последствий, разработка и внедрение в АСУДС многоуровневой системы обеспечения информационной безопасности выходит на первый план.

СПИСОК ЛИТЕРАТУРЫ

1. Нырков А.П., Нырков А.А., Соколов С.С., Шнуренко А.А. Обеспечение безопасности объектов информатизации транспортной отрасли. – СПб.: Изд-во Политехн. ун-та, 2015. - 544 с.
2. Нырков А.П. Безопасность информационных потоков в АСУДС / Нырков А.П., Викулин П.В. // Проблемы информационной безопасности. Компьютерные системы. – № 4, 2010. – С. 78 – 82.
3. Нырков А.П. Программно-аппаратная реализация системы предупреждения аварийной ситуации для объектов морского транспорта / А. П. Нырков, А. А. Жиленков, С. С. Соколов, С. Г. Черный // Автоматизация в промышленности. – № 1, 2016. – С. 26 – 30.
4. Люльченко А.Н. Модель системы обеспечения информационной безопасности на транспорте / А. Н. Люльченко, А. П. Нырков, В. Г. Швед // Вестник государственного университета морского и речного флота имени адмирала С.О. Макарова, № 5 (33), 2015. – С. 184 – 193.
5. Нырков А.П. Информационные технологии в обеспечении безопасности судоходства на внутренних водных путях / Нырков А.П., Нырков А.А. // Материалы конференции «XIV Санкт–Петербургская международная конференция «Региональная информатика – 2014» (РИ–2014). – СПб.: СПОИСУ, 2014. – С. 279.
6. Вихров Н.М. О безопасности инфраструктуры водного транспорта / Н. М. Вихров, Ю. Ф. Каторин, А. П. Нырков, С. С.

Соколов, А. А. Шнуренко // Морской вестник. – № 4 (52), 2014. – С. 99–102.
7. Нырков А.П. О некоторых проблемах обеспечения информационной безопасности на внутренних водных путях Российской федерации / Нырков А.П., Нырков А.А. // Материалы конференции «XIV Санкт–Петербургская международная конференция «Региональная информатика – 2014» (РИ–2014). – СПб.: СПОИСУ, 2014. – С. 280 – 281.
8. Нырков А.П. Обеспечение безопасности автоматизированных систем управления движением судов при помощи технологии референцных станций / А. П. Нырков, С. С. Соколов, Н. Ю. Вайгандт // Морская радиоэлектроника. – № 2 (44), 2013. – С. 48 – 50.
9. Бухарметов М.Р. Комплексная система обеспечения информационной безопасности автоматизированных систем на водном транспорте: материалы конференции «Современные тенденции и перспективы развития водного транспорта России» – СПб.: Изд-во ГУМРФ им. адм. С.О.Макарова, 2017. - 624 с.

УДК: 004.4

ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ РАБОТЫ ДОБЫВАЮЩИХ СКВАЖИН

Вирстюк Анастасия Юрьевна, Микшина Виктория Степановна, Ельмендеев Алик Питибаевич
Сургутский государственный университет
e-mails: Nastua5.1991@mail.ru, mikshinavs@gmail.com, alikelm@icloud.com

Аннотация. В работе рассмотрены существующие гидродинамические и промыслово-статистические модели, применяемые для анализа эффективности работы добывающих скважин, выделены проблемы их применения в современных условиях нефтедобычи и предложено создание адаптационных геолого-промысловых моделей, учитывающих современное состояние добывающих скважин.

Ключевые слова: *добывающие скважины; эффективность; регрессия.*

USING MATHEMATICAL MODELS IN THE ASSESMENT OF THE EFFICIENCY WORK OF OIL WELLS

Anastasiya Virstyuk, Viktoria Mikshina, Alik Elmendeev
Surgut State University
e-mails: Nastua5.1991@mail.ru, mikshinavs@gmail.com, alikelm@icloud.com

Abstract. The paper deals with current hydrodynamic and industrial statistical models for analyses of the efficiency work of oil wells. Also, problems of their using in the modern oil recovery are highlighted and it is proposed the creation of adaptive geological industrial models considering the modern state of oil wells.

Keywords: *oil wells; efficiency; regression.*

Финансовая устойчивость нефтегазодобывающего предприятия в значительной степени зависит от эффективного использования фонда добывающих и нагнетательных скважин.

Для определения эффективности их работы требуется изучение большого количества показателей: дебит, приемистость, обводненность продукции и т.п. Кроме того, по мере разработки месторождений появляется потребность в анализе трудноизвлекаемых запасов нефти, запасов с высокой степенью выработанности, профиля приемистости и притока скважин и т.п., что приводит к появлению новых параметров, характеризующих работу скважин. Вследствие анализа ограниченного количества показателей и отсутствия учета новых, существующие математические модели эффективности работы скважин недостаточно адекватно описывают реальное положение дел на месторождениях.

Промыслово-статистические и адаптационные модели. Для оценки и прогнозирования показателей разработки скважин (и как следствие эффективности их работы) были разработаны промыслово-статистические методы прогноза, применение которых очень важно особенно на поздних стадиях разработки месторождений.

На данный момент разработано более 40 промыслово-статистических методов прогноза показателей разработки. Разработанные методы описываются кривыми вытеснения.

Промыслово-статистические методы прогноза характеризуются оперативностью (экспрессностью), простотой; основываются на минимальном количестве исходных данных. Но с другой стороны, промыслово-статистические методы характеризуются рядом отрицательных черт. Во-первых, при применении экстраполяционных методов погрешность оценки показателей разработки возрастает с ростом промежутка экстраполяции. Во-вторых, на ранних стадиях разработки методы характеризуются низкой результативностью, так как показатели разработки не обладают необходимой долей стационарности (поэтому применение кривых вытеснения обоснованно только при обводненности более 50%). В-третьих, все кривые вытеснения получены эмпирическим путем на основе обобщения промысловых данных ограниченного количества месторождений, вследствие чего они могут быть не вполне корректны для месторождений (скважин), имеющих другие особенности работы. В-четвертых, для построения аппроксимационной зависимости выбирается ограниченный прямолинейный участок кривой, но не менее 5-6 и не более 10-12 точек. И, наконец, в – пятых, объективных критериев отбора характеристик не существует, расчет ведется как минимум по 3 зависимостям, по которым коэффициент детерминации наиболее близок к 1.

Поэтому в настоящее время всё большее внимание обращено на адаптационные геолого-промысловые модели (АГПМ), которые могут быть подобраны для скважин с любыми характеристиками и условиями работы. Благодаря этим моделям осуществляется анализ за короткий промежуток времени (в отличие от геолого-промысловых методов), поэтому экстраполяционная ошибка не накапливается. Но следует отметить, что даже для одного и того же параметра (к примеру, для нефтедобычи) уравнение регрессии, на основе которого и строятся АГПМ, может приобретать различный вид, так как пласты и скважины имеют различные эксплуатационные характеристики – обводненность более или менее 50%, однородность или неоднородность, малая или высокая вязкость нефти и т.д

Таким образом, адаптационные геолого-промысловые модели являются очень трудоемкими, и их применение возможно и целесообразно в рамках программных средств, благодаря которым будет проводиться предварительный анализ геолого-технических параметров скважин и подбираться необходимая модель и соответствующее ей уравнение регрессии. Кроме того, АГПМ позволяют определить зависимость одного нефтепромыслового параметра от нескольких других, что является необходимым для комплексного анализа работы скважины, в частности, для определения эффективности работы, которая для нефтяных и нагнетательных скважин может складываться из различных характеристик (к примеру, распределение закачки по пластам, профиль приемистости и т.п.), а не только на основании дебита или приемистости.

Для оценки существующих промыслово-статистических и разрабатываемых адаптационных геолого-промысловых моделей был произведен следующий анализ. Для одной и той же скважины X с определенными соотношениями Q нефти (Qн) и Q жидкости (Qжид) сначала были построены две промыслово-статистические зависимости (по Камбарову и Сазонову).

В случае с АГПМ для анализа скважин с различными эксплуатационными характеристиками требуется разбить все исследуемые скважины на группы (провести так называемую классификацию) для того, чтобы подобрать определенный вид уравнения регрессии для каждой из них.

Для определения эффективности работы добывающей нефтяной скважины необходимо провести анализ дебита скважины и дополнительных показателей:

1. Геолого-физические: вязкость и плотность пластовой нефти, пластовая температура, содержание парафинов, пористость и проницаемость пласта, коэффициент вариации нефтенасыщенности, толщина пластов и пропластков, коэффициенты неоднородности, песчанистости и расчлененности пласта, относительные запасы нефти.

2. Технологические: темпы отбора жидкости, соотношение закачки и отбора жидкости, плотность сетки скважин и интерферирующие нагнетательные скважины, текущие запасы нефти на скважину.

Скважину X, рассматриваемую в качестве примера, можно определить к группе скважин с маловязкой нефтью и однородным объектом разработки. Вязкость пластовой нефти этой скважины составляет не более 5 МПа*с, комплексный коэффициент неоднородности не более 6.

Учитывая всё вышесказанное, можно определить уравнение множественной регрессии для скважин с маловязкой нефтью и однородным пластом: эффективность работы скважины в данном случае будет зависеть от вязкости нефти, толщины пропластков и комплексного коэффициента неоднородности.

Оценка адекватности рассматриваемых моделей проводилась с помощью F-критерия Фишера. И в первом, и во втором случаях построенная регрессия является значимой, но при использовании адаптационной геолого-промысловой модели коэффициент детерминации составляет 99%, а для промыслово-статистических моделей порядка 95%. Соответственно анализ дополнительных показателей работы скважин позволяет дать более точную и правильную оценку эффективности работы добывающих скважин и соответствует современным условиям процесса нефтедобычи на месторождениях.

СПИСОК ЛИТЕРАТУРЫ

1. Вирстюк А. Ю. Разработка модуля по контролю нагнетательных скважин с неравномерным профилем приемистости // Север России:стратегии и перспективы развития: материалы II Всерос. науч-практич.конф. 2016. С. 140.
2. Вирстюк А. Ю. Пространственное распределение объемов закачки по пластам // Север России:стратегии и перспективы развития: материалы III Всерос. науч-практич.конф. 2017. С. 169.
3. Григулецкий В.В. Обводнение месторождений - коренной вопрос современности российской нефтегазовой отрасли [Электронный ресурс] //Технологии ТЭК. 2007 URL:http://www.oilcapital.ru/edition/technik/archives/technik/technik_02_2007/108204/public/108222.shtml (дата обращения: 29.04.2017).
4. Гамилова Д.А., Буренина И.В. Управление фондом скважин на основе комплексной оценки эффективности их эксплуатации [Электронный ресурс] // Электронный научный журнал «Нефтегазовое дело». 2007. N1. URL: http://ogbus.ru/authors/Gamilova/Gamilova_1.pdf. (дата обращения: 21.04.2017).
5. Токарев М.А., Чинаров А.С. Статистические методы прогноза нефтеотдачи и оценки эффективности воздействия на пласт: учеб.пособие. Уфа: ООО «Монография», 2007.

УДК: 004.78

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УПРАВЛЕНИИ ТРАНСПОРТОМ ГОРОДА, КАК ЭЛЕМЕНТ РЕАЛИЗАЦИИ КОНЦЕПЦИИ «УМНОГО ГОРОДА»

Жигадло Валентин Эдуардович
Филиал ФГУП ЦНИИС – ЛО ЦНИИС
194223, Россия, Санкт-Петербург, ул. Варшавская, 11
e-mail: zve@mail.ru

Аннотация. В современных условиях эффективность процесса управления жизнедеятельностью современных мегаполисов, в частности, определяется наличием и качеством используемых информационных систем управления транспортной инфраструктурой. В докладе подробно рассматриваются принципы построения подсистемы управления транспортной инфраструктурой мегаполиса, как составной части в реализации концепции «Умного Города».

Ключевые слова: *безопасный город; умный город; управление транспортом; информационная система.*

INFORMATION SECURITY IN MANAGEMENT OF CITY TRANSPORT, AS THE ELEMENT OF IMPLEMENTATION OF THE CONCEPT OF "THE CLEVER CITY"

ZhigadloValentin
Federal State Unitary Enterprise TSNIIS branch – LO TSNIIS
194223, Russia, St. Petersburg, Varshavskaya str., 11
e-mail: zve@mail.ru

Abstract. In modern conditions efficiency of process of management of activity of modern megalopolises, in particular, is defined by existence and quality of the used information management systems transport infrastructure. In the report the principles of creation of a subsystem of management of transport infrastructure of the megalopolis as component in implementation of the concept of "the Clever City" in detail are considered.

Keywords: *safe city; smart city; management of transport; information system.*

Система управления транспорта мегаполиса создается с целью обеспечение повышения качества реализации управляющих воздействий в функционировании транспортного комплекса агломерации, независимо от ведомственной принадлежности элементов транспортного комплекса, особенно в условиях возникновения нештатных ситуаций, имеющих высокую социальную значимость.

Система управления транспортом предназначена для решения следующих задач:

1. Мониторинг функционирования транспортного комплекса города в режиме реального времени, включая: работу городского пассажирского транспорта общего пользования (наземного и метрополитена) независимо от его принадлежности; работу пассажирских терминалов «внешнего» транспорта (аэропорт, железнодорожные вокзалы, морские, речной и автобусные вокзалы); условия движения на улично-дорожной сети агломерации на основе информации локальных АСУ ДД (интеграционного центра АСУДД); функционирование системы парковочного пространства города; работу спецтехники, выполняющей работы по обслуживанию УДС; закрытия улично-дорожной сети; контроль за перевозкой крупногабаритных, тяжеловесных и опасных грузов; работу транспорта специальных городских служб (аварийных, МЧС, полиции и т.д.); в перспективе мониторинг полетов воздушных судов на горизонтах ниже нижнего.
2. Обеспечение координации работы различных элементов транспортного комплекса города, включая координацию: работы городского наземного пассажирского транспорта общего пользования и метрополитена между собой; работы городского наземного пассажирского транспорта общего пользования и метрополитена с «внешними» видами пассажирского транспорта (воздушный, железнодорожный, морской, речной, автобусный); работы транспорта специальных городских служб (аварийных, дорожных, МЧС, полиции и т.д.); работы различных АСУ ДД, функционирующих в агломерации с работой центра управления парковочным пространством; работы различных АСУ ДД, функционирующих в агломерации с работой диспетчерских центров управления пассажирскими перевозками.
3. Прогнозирование развития транспортной ситуации при возникновении экстренных событий и нештатных ситуаций, включая прогнозирование: возникновения «критических» заторов на УДС; сбоев в работе наземного пассажирского транспорта общего пользования (в т.ч. электротранспорта); сбоев в работе метрополитена; возникновения нештатных ситуаций на терминалах «внешнего» пассажирского транспорта; возникновения нештатных ситуаций при перевозке опасных и негабаритных грузов и их последствий.
4. Мониторинг полетов воздушных судов на горизонтах ниже нижнего.
5. Оперативное реагирование в нештатных ситуациях, включая: анализ возможных нештатных ситуаций, требующих изменения работы ТК (отдельных элементов ТК); типизацию нештатных

ситуаций и критериев их идентификации; оперативное распознавание (определения) нештатных ситуаций; оперативные действия по транспортному обеспечению в нештатных ситуациях на основе разработанных регламентов принятия решений в нештатных ситуациях их реализации.

6. Взаимодействие с другими (внешними) системами, штабами, центрами, включая: городской мониторинговый центр; центры управления (диспетчерские центры) служб МЧС, полиции; центры управления (диспетчерские центры) городских коммунальных служб;

7. Предоставление информационных сервисов исполнительным органам города и гражданам, включая: обобщенную (интегрированную) информацию по работе наземного пассажирского транспорта общего пользования и метрополитена; информацию об условиях движения на улично-дорожной сети города, об экстренных событиях и нештатных ситуациях в работе транспортного комплекса и прогнозируемых сроках их устранения; краткосрочные прогнозы по изменению транспортной ситуации в городе.

В докладе подробно рассматриваются особенности построения современных уже существующих систем управления транспортом, а также существующие подходы для организации управления отдельными областями жизнедеятельности крупных мегаполисов (безопасностью жизнедеятельности (КСОБЖН), обеспечением правопорядка (АПК «БГ»)) предлагается решение по построению СУ мегаполисом на принципах архитектуры системы «Smart Sity».

СПИСОК ЛИТЕРАТУРЫ

1. Резолюция 4-й конференции «Система распределенных ситуационных центров − 2014», 16−17 октября, г. Воронеж.
2. Резолюция 5-й конференции «Система распределенных ситуационных центров», 7-9 октября 2015 г., г. Ярославль.
3. Концепция построения и развития аппаратно-программного комплекса «Безопасный город», утвержденная распоряжением Правительства Российской Федерации №2446-р от 03 декабря 2014 года;
4. Наставление по организации деятельности центров управления в кризисных ситуациях МЧС России, Москва, 2012 г.
5. В. Чернышев. Инфраструктура «Умного Города» - оптимальные решения, CNews Conferences, Москва, 2013 г.

УДК 004.056

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОРСКИХ ТРАНСПОРТНЫХ СИСТЕМ

Константин Петрович Голоскоков[1], Марина Юрьевна Чиркова[2]
[1] Государственный университет морского и речного флота имени адмирала С.О. Макарова
Россия, Санкт-Петербург, ул. Двинская, 5/7
[2]Санкт-Петербургский государственный экономический университет
Россия, Санкт-Петербург, Садовая ул., 21
e-mails: kpg777@rambler.ru, mu.tch@mail.ru

Аннотация. Рассмотрены проблемы обеспечения информационной безопасности морских транспортных систем и способы их решения.

Ключевые слова: *информационная безопасность; транспортные системы; угрозы; риски.*

PROBLEMS OF INFORMATION SECURITY OF MARITIME TRANSPORT SYSTEMS

Goloskokov Konstantin[1], Chirkova Marina[2]
[1] Admiral Makarov State University of Maritime and Inland Shipping
Russia, St. Petersburg, Dvinskaystr., 5/7
[2]St. Petersburg State Economic University
Russia, St. Petersburg, Sadovaystr., 21
e-mails: kpg777@rambler.ru, mu.tch@mail.ru

Abstract. The article considers the problems of ensuring information security of the Maritime transport systems and their solutions

Keywords: *information security; transportation systems; threats; risks.*

В большинстве важных отраслей, таких как, например, энергетическая, огромное внимание уделяется информационной безопасности, а транспортная отрасль значительно отстает в этом вопросе.

Проблема заключается в том, что никогда прежде транспортная отрасль не придавала большого значения увеличению производительности информационных систем и в то же время их эффективности. Эффективность в этом случае означает улучшение финансовой отдачи и сокращение потребления ресурсов.

Таким образом, в этой сложной системе судов морского транспорта нужно улучшить безопасность систем (ICS-Security-for-Public-Transportation-Systems).

Тенденции глобальной урбанизации оказывают влияние на системы морских перевозок для увеличения пропускной способности и повышения эффективности, а применение сетей Ethernet увеличивает информационные угрозы.

Для увеличения производительности и мощности морских транспортных систем используют достижения в области информационных технологий.

Это неизбежно означает переход от традиционных устаревших систем использующих автономное индивидуальное оборудование к более широкому использованию стандартизированных технологий, протоколов и операционных систем (например, Ethernet).

Эти новые технологии обычно имеют открытые интерфейсы и стандартизованные протоколы. Так-как они все чаще применяются в системах управления и связи, увеличивается риск кибератак на транспортные информационные системы.

Кроме того, повышается уровень обслуживания клиентов и взаимосвязь между ранее существовавшими автономными системами.

Для осуществления взаимосвязи используются выделенные линии связи, которые также приводят к риску нарушения информационной безопасности.

Информационная безопасность имеет большое значение, несмотря на применение отказоустойчивых методологий, применяемых в транспортной отрасли.

Кроме того, по мере того, как операционные системы становятся более сложными, достичь надежных отказобезопасных условий труднее.

Особенно когда операционные системы подвергаются преднамеренной кибератаке.

Также важно отметить, что кибер-риски не ограничиваются безопасностью. Информационная безопасность может повлиять на всю цепочку транспортных перевозок Неудачи в цепочке поставок, особенно те, которые сохраняются в течение нескольких дней, быстро окажут прямое воздействие на работу всей транспортной системы.

Существуют также коммерческие риски, особенно когда нападения оказывают непосредственное влияние транспортные услуги. Наконец, интерес средств массовой информации к информационной безопасности может оказать большое влияние на доверие к морским транспортным системам.

Основные рекомендации по информационной безопасности могут быть сформулированы в следующей последовательности:

– провести оценку риска; нужно понять, как выглядит сеть и где находятся критические точки.

– создание плана по защите сети, используя собранные знания экспертов в этой области, подход, который можно предпринять, называется Defense in Depth (DiD), что означает множественные уровни защиты, распределенные по всей сети.

Хорошо разработанная стратегия DiD включает в себя несколько уровней защиты вместо того, чтобы полагаться на единую точку безопасности.

Дифференцированные уровни защиты, гарантируют, что злоумышленник не сможет получить доступ ко всем последующим слоям после прохождения первого слоя. Каждый уровень оптимизирован для борьбы с определенным классом угрозы.

Если сеть защищена стратегией DiD, последствия случайного инцидента с безопасностью или злоумышленной атакой будут ограничены зоной, в которой возникла проблема.

– защитить критические точки, определить приоритетность критических точек, которые могут привести к полной катастрофе для сети.

Основные проблемы информационной безопасности систем морского транспорта связаны с высокой стоимостью оценок рисков, что не позволяет эффективно защищать транспортные системы.

Для решения этой проблемы необходимо выбрать многоуровневый подход определения приоритетности наиболее важных точек, в которых можно успешно внедрить хорошие средства киберзащиты.

СПИСОК ЛИТЕРАТУРЫ

1. Голоскоков К. П. Формирование информационной базы для прогнозирования качества продукции / К. П. Голоскоков // Инновации. — 2009. — № S1. — С. 91–94.
2. Голоскоков К.П Прогнозирование технического состояния изделий судовой электронной техники. ООО «ПаркКом», Санкт-Петербург, 2007. 148 с.
3. Ныркова А.П. Обеспечение безопасности объектов информатизации транспортной отрасли / под ред. А. П. Ныркова. / А. П. Нырков, А. А. Нырков, С. С. Соколов, А. А. Шнуренко // СПб.: Изд-во Политехн. ун-та, 2015. – 544 с.
4. Нырков А.П., Соколов С.С., Башмаков А.В. Методика проектирования безопасных информационных систем на транспорте // Проблемы информационной безопасности. Компьютерные системы. – 2010. –№ 3. – С. 58–61.
5. Люльченко А.Н. Модель системы обеспечения информационной безопасности на транспорте / А. Н. Люльченко, А. П. Нырков, В. Г. Швед // Вестник государственного университета морского и речного флота имени адмирала С.О. Макарова, № 5 (33), 2015. – С. 184 – 193.

УДК 070.12 (070.13, 070.481)

ФЛЕШ-МОБ КАК ПРОТЕСТНАЯ ТЕХНОЛОГИЯ В ПОЛИТИЧЕСКОМ ДВИЖЕНИИ (НА ПРИМЕРЕ УКРАИНЫ)

Дегтярева Ольга Викторовна
Северо-Западный институт управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации
Россия, Санкт-Петербург
e-mail: olgaspb2008@mail.ru

Аннотация. Нынешнее состояние СМИ Украины вызывает серьезные вопросы относительно того, являются ли справедливыми и сбалансированными проведенные избирательные компании. Сложная система цензуры, в том числе инструкции, исходящие от финансово-промышленных групп, искажают новости и освещение политических дел. Рассматриваются тенденции и перспективы развития информационного общества, связанные с возникновением и широким распространением социальных сетей. Анализируются социальные, политические и этические аспекты сетевой коммуникации. Раскрываются особенности организации и проведения мероприятий политического флеш-моба, определение его как инструмента политического консьюмеризма.

Ключевые слова: *флеш-моб; фан-моб; симулякр-моб; смарт-моб; Евромайдан.*

FLASH-MOB AS A PROTEST TECHNOLOGY IN THE POLITICAL MOVEMENT (ON THE EXAMPLE OF UKRAINE)

Degtiareva Olga
Russian Presidential Academy of National Economy and Public Administration (RANEPA)
Russia, St. Petersburg
e-mail: olgaspb2008@mail.ru

Abstract. The current state of Ukraine's media raises serious questions as to whether a fair and balanced electoral contest can be held. An elaborate system of censorship, including instructions emanating from the financial and industrial groups, distorts news and skews coverage of political affairs. The author discusses tendencies and perspectives of the development of the information society related to the emergence and expansion of social networks. Social, political and ethical aspects of Internet communication are analyzed. Features of the organization and carrying out of actions political flesh-mob, its definition as tool political consumerism are revealed.

Keywords: *flesh-mob; fan-mob; simulacrum-mob; smart-mob;Euromaidan.*

Введение. После событий «Революции достоинства» или Евромайдана формы социального протеста в украинском обществе приобрели черты провокативности. Именно благодаря новым медиа в конце 80-х-начале 90-х г. XX в. в поле публичного обсуждения попали такие понятия, как «самоидентификация» и «право на самоопределение» [18], а политические события, связанные с этими понятиями, стали на долгие годы предметом ярких и острых медийных дискуссий. Сетевые ресурсы помогали различным сообществам, ориентированным на радикальные изменения в общественной жизни, переводить эти дискуссии в практическую плоскость, способствовали самоорганизации сообществ, осуществляли мобилизацию [6] или в целях проведения политических акций, постановочных мероприятий (флеш-мобов) или демобилизацию [7].

Сетевые СМИ вызвали к жизни инновационные формыпротестной активностимолодежи (флешмоб, хеппенинг, перформанс, наномитинг), «обусловленные трендами постмодернизма, глобализационными процессами, стремительным развитием информационных технологий и коммуницирования акторов политического процесса» [1]. Флеш-моб становится моделью нового политического действия [13].

С начала XXI в. медиактивисты стали использовать сетевые медиа для борьбы с гегемонией, репрессиями, эксплуатацией и корпоратизацией [4, 6]. Появилось огромное количество информационных материалов, наполненных не только идеями протеста, инакомыслия и бунта, но и призывами к конкретным политическим действиям [3-5].

Связи в социальных сетях показывают, как спонтанны и хаотичны могут быть социальные образования без конструктивного лидера, как дух толпы и призывы к реальным действиям способны затмить изначальную повестку дня. Благодаря социальным сетям создается своеобразная «коммуникативная автономия» [19, С. 198]. Медиаактивисты ставят перед собой следующие задачи:

1) управление контентом «лояльных СМИ»;

2) блокировка независимых СМИ с целью остановки генерирования мобилизационного контента протестного движения;

3) инициирование контента в нелояльных сообществах и блогах (сетевой троллинг);

4) инициирование и распространение контента в лояльных блогах и сообществах [8].

На сегодняшний день большая часть протестных движений, имеющих цель изменить мышление людей, ориентированы на долгосрочный результат. Медиаактивисты указывают стратегические цели, такие как: формирование общественного мнения; создание групп сторонников, создание сети оповещения и механизмов быстрого реагирования; реализация программ тренировок активистов, привлечение специалистов (реклама, маркетинг, социальные работники, администрация), чьи знания и опыт будут полезны для проведения акций и мероприятий; наращивание волны общественного мнения, поддержка интереса к волнующим вопросам, показ безысходности ситуации, предлагаемое единственное решение [2, 6, 7].

Решаются и тактические задачи: выведение локальной общественной проблемы в публичную сферу, ее обострение, работа с лидерами местного общественного мнения, имеющими ресурс влияния на людей, которых непосредственно затрагивает данная проблема; организация акций (перекрытие дороги, блокирование зданий органов власти и транспортных средств чиновников, вывешивание транспарантов на административных зданиях); создание информационных поводов; прямое гражданское давление на нелояльные СМИ.

Флеш-мобы используют два вида пространств для взаимодействия членов сообществ – киберпространство и городскую среду (улицы, пощади). В мире накопился дефицит демократии, а это означает, что граждане не доверяют своим представителям во власти. Социальные медиа радикализируют протест. Возникновение стихийного движения, новой формы коллективного существования политического активизма, организованного с помощью сетей, без лидеров, без политических организаций, состоящее из людей, которые больше не могут принимать несправедливость в обществе, это новая и важная форма гражданского общества, которое проявляет себя в этом контексте.

Государства, в которых присутствуют даже незначительные зачатки демократического процесса, а также есть Интернет, наверняка будут подвергнуты «запросу на демократию снизу». Современные ученые считают, что такие изменения являются четкими предпосылками появления нового посткультурного, «предцифрового» века с новыми формами медиаактивизма, отражающего интервенционистские медиа-арт-практики [4], так называемые hitand-run вмешательства в медийную сферу с использованием новых технологий от bio-арта и science-арта до сетевого искусства и тактических медиа [2, 5]. Бизнес-модель, лежащая в основе традиционных СМИ, изжила себя. То есть мы имеем своеобразную точку бифуркации, в которой соединились массовая гражданская журналистика и элементы демократии [9, 11, 12], [16, С. 95].

Рассматривая конвенциональные формы политического членства в социально-политических организациях в Украине, нельзя не заметить привлечение, рост интереса и активное участие населения Украины в неформальных акциях и практиках [13, 18]. В Украине первым флеш-мобом принято считать 16 августа 2003 г., когда в киевском ТК «Глобус» на Площади Независимости собралось полтора десятка молодых людей в черных очках, которые хлопали в ладоши и фотографировали «объект пальму» [15]. К таким же движениям можно отнести, например, движение антиглобалистов, «еврооптимистов», сбор петиций, спонтанные акции протеста, которые не требуют членства в каких-либо организациях. Эта проблематика непосредственно связана со сферой политического консЮмеризма как политически мотивированного потребительского поведения граждан. Сегодня политический консюмеризм характеризует новые тенденции политической активности населения Украины, в частности, молодежи. Граждане избегают членства в партиях и участия в голосованиях [15]. На смену традиционным формам политической активности пришли новые способы социального взаимодействия. Более востребованными стали такие коллективные действия, которые характеризуются спорадичным способом мобилизации населения, а также неиерархичные и менее формализованные движения [17, 19]. Одной из таких форм являются флеш-мобы (в переводе с англ. flash-mob – мгновенная толпа). Суть флеш-моба состоит в неожиданном появлении какого-то количества людей в одном месте, которые заранее договорились с помощью СМК, осуществить определенное запланированное мероприятие.

Организация флеш-мобов предполагает следующую последовательность действий [3]: 1) разработка сценария акции и ее размещение на веб-сайте или рассылка сообщений с целью привлечения людей; 2) обсуждение сценария мероприятия; 3) появление людей на месте проведения акции; 4) появление лидеров или людей, которые должны дать условный сигнал к началу акции; 5) активизация толпы; 6) групповые активные действия; 7) окончание акции и мгновенное рассеивание участников акции в толпе прохожих; 8) обсуждение результатов акции на веб-сайтах.

Исследователи классифицируют флеш-мобы ПО разным критериям, а именно: масштабу проявления: глобал-моб (охватывает несколько городов или стран) и моб (одноразовая акция в одном городе); направлению акции: арт-моб (искусство), соушл-моб (социальное или политическое направление) и моб (развлекательное направление); среде проявления: I-моб (акция, которая проводится в Интернете), sms-моб (акция, которая проводится с помощью смс-сообщений в телефонах пользователей мобильной связи), реал-моб (акция в реальном измерении); целевому назначению: фан-моб (как развлечение), симулякр-моб (имитация флеш-моба в коммерческих целях) и смарт-моб (флеш-моб идеологической направленности) [13, С. 172].

Флеш-моб активно развивается в качестве развлечения для молодежи (фан-моб), а также как симулякр (как явление, которое имитируется с определенной целью). Симулякр-моб является методом практического использования флеш-моба в рекламных целях, а именно в партизанском маркетинге, основой которого является выход за границы общепринятых способов и методов рекламных коммуникаций и продвижения товара.

Следует отметить, что изначально флеш-моб не был предназначен для политических или PR-акций – все участники, как правило, не были знакомы или объединены между собой. Более того, использование акций флеш-моба для достижения политических целей было запрещено установочными правилами. Предполагалось, что флеш-моб является свободным самовыражением и акцией искусства, а не способом политического давления. Флеш-моб планировался как своеобразный способ социального протеста путем абсурдизации. Очевидно, что такая эффективная форма выражения идей не могла оказаться вне поля зрения политических сил. Впервые как политическая акция флеш-моб состоялся 30 ноября 1999 г., когда люди скоординировали свои действия с помощью мобильных телефонов и сети Интернет и самостоятельно образовали столпотворение против проведения встречи ВТО (Всемирной Торговой Организации) («Битва за Сиетл») [10].

В Украине политические флеш-мобы представлены симулякр-мобами и смарт-мобами [13]. Первый способ используется как политическая технология и рекламная акция определенной политической силы, а смарт-моб – как самоорганизующееся и добровольное объединение граждан с целью выражения отношения к власти, политической системе и пр. Возможно также объединение этих двух форм флеш-моба. Одним из примеров такого объединения выступает «Оранжевая революция» 2004 г. Среди примеров менее масштабных можно назвать акцию, которая состоялась 22 ноября 2009 г. в г. Днепропетровск (в настоящее время переименован в г. Днепр), которую проводила Украинская народная партия под лозунгом «Покупай украинское! Защищай украинское, так как это твое!» [13, С. 172]. Подобные акции неоднократно повторялись и позже. Несмотря на то, что флеш-моб зародился как аполитическая акция, в нем заложен значительный политический потенциал. В первую очередь, он состоит в реализации механизма позиционирования определенной политической силы или движения. Естественно, флеш-мобы в Украине получили особое распространение среди оппозиционных политических сил не только потому, что позволяют скрывать настоящий смысл акций и снижают потенциал преследований участников властными структурами. Еще одна причина – в том, что действующая власть не должна позиционировать себя через несерьезные политические акции, которые когут негативно отразиться на имидже [11].

Основой современного политического флеш-моба выступает так называемая «умная толпа» [10], возможности которой усилились с развитием компьютерных технологий и устройств. Политический флеш-моб, организуемый сетевыми медиа, – это не просто интеллектуальное развлечение, которое присутствует в традиционном флеш-мобе. Он имеет конкретную цель – смена политического режима и импульс «цветной революции».

Заключение. На сегодняшний день флеш-моб оправдывает себя как эффективная технология, способная привлечь большое количество людей, которые свободно владеют современными средствами связи. Участие в подобной акции более привлекательно в сравнении с традиционными формами общественных сборов. Плюсы очевидны: флеш-моб требует меньше времени, участие в нем анонимно, проходит без предварительной подготовки и похож на квест или игру, что нравится особенно молодежи. Флеш-моб представляет собой слабо формализованные, неирерархичные, спорадические по способу мобилизации коллективные действия, которые являются действенным инструментом политического консюмеризма. Остается открытым вопрос о том, насколько безопасен флеш-моб, ведь он позволяет собрать огромную толпу буквально в считанные часы.

СПИСОК ЛИТЕРАТУРЫ

1. Авцинова Г.И., Воронина Е.Ю. Инновационные формы протестной активности молодежи [Электронный ресурс] / Г.И. Авцинова, Е.Ю. Воронина // PolitBooK. – 2014. – № 3. –URL: https://cyberleninka.ru/article/n/innovatsionnye-formy-protestnoy-aktivnosti-molodezhi (дата обращения: 04.12.2016).
2. Беспалов М. Флешмоб как метод художественного сознания [Электронный ресурс] / М. Беспалов // Флешмоб — феномен управляемой толпы. URL: http://mobs.alfamoon.com/flashmob–articles/flashmob–as–art.html (дата обращения: 16.01.2017).
3. Искусство создавать акцию: Межрегиональная молодежная общественная организация «Новые Люди». (г. Волгоград 2007 год). [Электронный ресурс] // URL: http://pandia.ru/text/77/217/4372.php (дата обращения: 17.01.2017).
4. Мельник Г.С., Мисонжников Б.Я. Дисфункция медийного дискурса или к поиску «перформативности» тактических медиа [Электронный ресурс] / Г.С. Мельник, Б.Я. Мисонжников // Мир лингвистики и коммуникации: электронный научный журнал. – 2014. – № 2. – С. 24 – 32. – URL: http://tverlingua.ru (дата обращения: 23.12.2016).
5. Мельник Г. С. Тактические медиа в деструктивных технологиях протеста / Г.С. Мельник // Вестник Санкт-Петербургского университета. Серия 16, Психология. Педагогика. – 2015. – Вып.3. – С. 83-91.
6. Носик А.А. Публичные политические сетевые институции и процессы мобилизации: сетевой анализ протестного ядра и его формирования / А.А. Носик // Век информации. – 2017. – № 2. – С. 111-113.
7. Томин Л.В. Интернет и социальные медиа как инструмент политической мобилизации. Дискуссии о трансформации политических организаций и антисистемных движений / Л.В. Томин // Век информации. – 2017. – № 2. – С.116-117.
8. Тюпина М. Э. Политическая демобилизация: понятие и технологии / М.Э. Тюпина // Век информации. 2017. – С.119-121.
9. Морозов Е. Интернет как иллюзия. Обратная сторона сети / Е. Морозов. – М.: АСТ, 2014. – 570 с.
10. Рейнгольд Г. Умная толпа: Новая социальная революция / Г. Рейнгольд. – М.: Фаир-пресс, 2006. – 416 с.
11. Сморгунов Л.В. Сетевые политические партии / Л.В. Сморгунов // Политические исследования. Полис. – 2014. – № 4. – С. 21-37.

12. Социальные сети и виртуальные сетевые сообщества: Сб. науч. тр. / Л.Н. Верченов, Д.В. Ефременко, В.И. Тищенко // РАН. ИНИОН. Центр социал. науч.-информ. исслед. Серия Информация. Наука. Общество. – М., 2013. – 360 с.
13. Шевчук И.Н. Флеш-моб как модель нового политического действия / И.Н. Шевчук // Вісник СевНТУ. Сер. Політологія: сб. науч. тр. — Севастополь, 2010. – Вып. 112. – С. 171–173.
14. Aslund A. Comparative Oligarchy: Russia, Ukraine and the United States / A. Aslund // Europe after the Enlargement». – Warsaw, April 8–9, 2005. – n 296. – 17 p.
15. Dyczok M. The politics of media in Ukraine: Election 2002. Ukraine at a Crossroads / M. Dyczok. - Bern: Peter Lang, 2005. – 250 p.
16. Jenkins H. Convergence: Where old and new media collide / H. Jenkins. – New York: New York University Press, 2006. – 308 p.
17. Kooiman J. Modern governance: New government-society interactions / J. Kooiman. – London: Sage, 1993. – 280 p.
18. Kuzio T., Wilson A. Ukrain: perestroika to independence / T. Kuzio, A. Wilson. – London: Macmillan; New York: St.Martin ' s Press, 1994. – 273 p.
19. Sorensen E., Torfing J. The Democratic Anchorage of Governance Networks / E. Sorensen, J. Torfing // Scandinavian Political Studies. – 2005. – №28(3). – PP. 195-218.

УДК 004.89, 007.52

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ИСПОЛЬЗОВАНИИ АВТОМОБИЛЬНОГО АВТОПИЛОТА

Кучеровская Олеся Владимировна
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, Большая Морская ул., 67
e-mail: kucherowskaya@gmail.com

Аннотация. Автомобили — это первый массовый продукт, в котором Искусственный Интеллект затронет каждого человека. Нейронные сети начали активно разрабатываться со второй половины XIX века и по сей день принимают главное участие в машинном обучении. Но чем дальше развиваются технологии, тем сложнее осуществляется киберзащита новых систем. Статья посвящена рассмотрению инновационных подходов к защите информации при использовании автомобильных автопилотов. В ней доказывается, почему необходимо уходить от использования стандартных математических алгоритмов при работе с поступающей информацией и использовать для защиты нейронную криптографию. Автор анализирует кибербезопасность автопилотных систем с нейросетевым обрабатывающим блоком.

Ключевые слова: *кибербезопасность; автомобильный автопилот; искусственная нейронная сеть; нейрокриптография.*

INFORMATION SECURITY WHEN USING AN AUTOMOBILE AUTOPILOT

Kucherovskaya Olesya
St. Petersburg State University of Aerospace Instrumentation
Russia, St. Petersburg, Bolshaya Morskaia str., 67
e-mail: kucherowskaya@gmail.com

Abstract. Cars are the first mass product in which the Artificial Intelligence will affect each person. Neural networks began to be developed actively from the second half of the 19th century and to this day take the principal part in machine learning. But new technologies become more difficult to be protected. The article is devoted to reviewing of innovative approaches to information security of automobile autopilots. In it is proved why it's necessary to avoid the use of standard mathematical algorithms by operation with the arriving information and to use neural cryptography. The author analyses cybersecurity of autopilot systems with the neural network processing block.

Keywords: *cybersecurity; automobile autopilot; artificial neural network; neurocryptography.*

В настоящее время мир переживает глобальные изменения. Прогресс требует создания инфраструктуры, основанной на интеллектуальных системах. Технологии должны стать основой для новых городов и интегрироваться в существующие. Чем больше объединяются умные технологии и города, тем сложнее процесс обеспечения безопасности обработки, хранения и доступности информации. В рамках студенческого проекта «Умный город» мной была рассмотрена сфера информационной безопасности.

За последние несколько лет в индустрии производства беспилотных автомобилей произошел невероятный прогресс. Приоритетной деятельностью для современных автопроизводителей является разработка такой системы для беспилотных автомобилей, которая во всех ситуациях на дороге будет принимать правильное решение почти со 100% вероятностью, а также будет обладать устойчивой киберзащитой. Чтобы гарантировать социальное принятие автоматизированных систем управления автомобилем, любые проблемы, которые касаются защиты информации и ответственности разработанных систем и решений, должны быть решены. Работоспособность и безопасность любого элемента системы может быть нарушена компьютерными атаками с использованием разного оборудования связи. Деструктивное воздействие на автопилот может быть осуществлено не только в криминальных, но и в террористических целях. Именно поэтому при

разработке автопилотных систем значительное внимание должно быть уделено информационной безопасности данных этих систем. С развитием технологий традиционным методам защиты становится все сложнее справляться со своими задачами, поэтому возникает необходимость поиска других.

Одним из перспективных направлений является применение искусственных нейронных сетей – нейрокриптография. Криптоанализ базируется на способности нейронных сетей исследовать количество наиболее подходящих решений. Также у них имеется возможность создавать собственные типы атак на существующие алгоритмы шифрования. Нейросистемы способны самообучаться, они не чувствительны к шуму, искажению данных, весовых коэффициентов, ошибкам в программе.

В разработке автомобильных автопилотов я предлагаю уйти от использования математических алгоритмов для обработки и защиты информации в автопилоте и начать использовать преимущественно нейронные сети — нейрокриптографию. Совершать внедрение в автопилот базовой нейронной системы, которая способна самостоятельно дообучаться и совершенствоваться.

Эффективность автопилота опеделяется способностью системы выполнять все поставленные задачи, используя минимум информации. Логические системы требуют больше датчиков (следовательно, возникает нагрузка большим объемом информации), так как для успешного выполнения алгоритов необходимы данные, строго соответствующие классификациям, которые были введены разработчиком. При использовании нейронных сетей в обучении автопилота, разметка для данных отсутствует. То есть у системы появляется возможность использовать все данные целиком, посколько разработчику не нужно вручную их размечать. Нейронная система может самостоятельно определить, какая именно информация ей необходима для выполнения задачи, считывать ее с датчиков и эффективно использовать. Нейросети способны распознавать объекты, расстояния до них с помощью анализа данных, поступающих с камер, не нуждаясь в помощи лидаров и радаров.

В каждом автопилоте есть входные устройства и датчики. Рассмотрим два автопилота: в первом обрабатывающим блоком является логическая система (рисунок 1), в другом — нейросеть (рисунок 2).

Рис. 1 Схема системы автопилота с логической системой управления

Рис. 2 Схема системы автопилота с нейронной системой управления

Изучив два набора датчиков, мы можем сделать следующий вывод. Если установить нейронную сеть, то для выполнения задачи понадобится меньше приборов. Самое главное преимущество — это то, что меньшее количество приборов позволит укрепить систему защиты информации. Если в логических системах необходимо обеспечивать безопасность пяти основных элементов автопилота, то в системах с нейронными сетями нужно защитить всего три. Это

уменьшает затратность процесса проектирования защитных систем и дает возможность более глубоко их проработать, позволяет оптимизировать процесс повышения безопасности системы автопилота. Радар и лидар являются наиболее уязвимыми подсистемами автопилота, так как их корректную работу можно нарушить без взлома самой системы. Они функционируют за счет излучения радиоволн и световых волн, которые можно сфальсифицировать или заглушить, тем самыс обманув автопилот. Подобные воздействия извне приводят к возникновению аварий. Отсутствие этих приборов повысит безопасность автопилота.

Логические системы (иначе говоря, символьные) основаны на знаниях. Они отлично работают в узких областях, но их явным недостатком является то, что они работают по конкретным условиям, которые заданы разработчиком. Они не способны дообучаться. Получается, что разработчик должен проектировать систему так, чтобы она покрывала как можно большее число случаев в реальном мире. А нейронным сетям достаточно набраться жизненного опыта, чтобы суметь превзойти в выполнении задач стандартные логические системы. Нейросети умеют создавать собственные методы шифрования, следовательно, взлом этих протоколов будет маловероятен. Нейронные сети могут научиться защищать конфиденциальность своих данных от других нейронных сетей: они обнаруживают формы шифрования и дешифрования, не обучаясь конкретным способам для выполнения этих целей. Стоит заметить, что нейронные сети могут также определить, что именно нужно шифровать, чтобы достичь выполнения задачи и максимизировать полезность. Криптография широко касается алгоритмов и протоколов, которые гарантируют тайну и целостность информации. Однако обучение нейросетей не требует предписания определенного набора криптографических алгоритмов, ни указания способов применить эти алгоритмы. Оно базируется только на постановке задачи — научиться самостоятельно совершать правильное решение, построив его антологию собственным способом, который человек не может предсказать. Обучаясь, нейросистема получает опыт, к которому она сможет обращаться в последующие разы. Так, она сможет запоминать приемы кибертатак и попытки обмана системы, и в последствии использовать наиболее эффективные методы противостояния им, но подстраиваясь под текущую ситуацию.

Таким образом, можно сделать вывод, что для повышения кибербезопасности автопилота необходимо использование нейронных сетей. Такие способности нейросистем, как самообучаемость, способность работать с большими объемами данных, решать даже плохо формализованные задачи и обращаться к собственному опыту, обеспечивают их превосходство по уровню результативности перед стандартными логическими системами защиты. За нейрокриптографией стоит будущее информационной безопасности автомобилей.

СПИСОК ЛИТЕРАТУРЫ

1. Гришин А.В. Нейросетевые технологии в задачах обнаружения компьютерных атак, 2011
2. Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н. и др., Применение искусственных нейронных сетей и системы остаточных классов в криптографии, 2012
3. Электронный журнал «Молодежный научно-технический вестник», 2014
4. https://m.geektimes.ru

УДК 004.9

АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОВ ПРОНИКНОВЕНИЯ В КОМПЬЮТЕРНУЮ СИСТЕМУ

Лукин Евгений Игоревич[1], Прокопович Максим Сергеевич[2]
[1] Санкт-Петербургский государственный экономический университет
Россия, Санкт-Петербург, ул. Садовая, 21
[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Россия, Санкт-Петербург, ул. Профессора Попова, 5
e-mails: genya.lukin@yandex.ru, mxm.prokopovich@gmail.com

Аннотация. В статье был проведен анализ современных угроз информационной безопасности, методов проведения целевых и массовых компьютерных атак. Были разобраны самые распространенные методы атаки на информационные системы, а также подробно исследована атака с использованием вредоносных макросов.

Ключевые слова: *вирусы; сети; проникновение; обратная разработка; программирование; уязвимости.*

ANALYSIS OF MODERNTHREATS AND THEIR METHODS OF PENETRATION INTO THE SYSTEM

Lukin Evgeny[1], Prokopovich Maxim[2]
[1] St. PetersburgState University of Economics "
Russia, St. Petersburg, Sadovaya str., 21
[2] St. Petersburg State Electrotechnical University «LETI»
Russia, St. Petersburg, Professor Popov str., 5
e-mails: genya.lukin@yandex.ru, mxm.prokopovich@gmail.com

Abstract. The article analyzes the current threats, attack methods, the structure of some of them, ways to protect the system from intruders. Were dismantled most common methods of attacks on information systems and investigated in detail the attack using malicious macros.

Keywords: *viruses; network penetration; reverse engineering; programming; vulnerability.*

Цель: показать существующие угрозы для информационных сетей, вывести общие принципы безопасной работы в сети и правила защиты объектов сетевой инфраструктуры.

Введение. В современных условиях при все большем распространении устройств, привязанных к глобальной сети, встает вопрос об их безопасности. Определить размах зараженных устройств почти невозможно. Следовательно, огромную роль играют средства защиты от проникновения зловредного агента в компьютерную сеть и его обнаружение.

В качестве примеров распространения вредоносного ПО на рабочие и домашние системы рассмотрим несколько векторов атак:

1. Перебор паролей для получения несанкционированного доступа к компьютерной системе. «Брутфорс» – способ взлома учётных записей в компьютерных системах, платёжных/банковских сервисах и на веб-сайтах посредством автоматизированного подбора комбинаций паролей и логинов. Брутфорс базируется на одноимённом математическом методе, в котором правильное решение – конечное число или символьная комбинация находится посредством перебора различных вариантов. Фактически каждое значение из заданного множества потенциальных ответов (решений) проверяется на правильность.

2. Распространение вредоносного ПОпосредством уязвимостей в операционных системах и программных продуктах. Данный способ распространения не подразумевает участия пользователя в процессе заражения системы, все уязвимые системы подвержены атаке. Уязвимости так же можно подразделить на известные сообществу и, напротив, еще не раскрытые широким массам. Большая опасность таится именно во втором типе уязвимостей, так как о них мало известно.

3. Фишинг. Данный тип подразумевает собой атаку непосредственно на пользователя. Зачастую фишинг атаки производятся на организации с целью заражения корпоративной сети с влекущие за собой противоправные действия в отношении объектов сетевой инфраструктуры компании и самой организации. Но такие атаки не ограничены корпоративным сегментом, рядовой пользователь тоже подвержен таким атакам. Именно этот вектор атаки в данный момент имеет наибольшую опасность, по причине малой осведомленности пользователей.

Брутфорс. Одной из угроз кибербезопасности в сети Интернет является ботнет – распределенная сеть зараженных компьютеров. Трудно определить размах ботнета и его основное расположение, так как все элементы распределены по всему миру. В 2016 по миру прокатилась волна крупных атак посредством ботнета Mirai и ботнетов, основанных на нем. И хоть размах атак был поистине колоссален, в основе системы заражения стоял примитивный перебор паролей по словарю. Сами же атаки были нацелены на «интернет вещей» (англ. Internet of Things — концепция вычислительной сети физических предметов, оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой посредством сети интернет).

Пример хранения паролей в ботнете mirai:

```
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10); //root xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9); //root vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8); //root admin
```

Mirai работает следующим образом: сканирует интернет в поисках уязвимых для брутфорса и взлома IoT-устройств, доступных через telnet. Вредоносное ПО поражает преимущественно камеры наблюдения, DVR и роутеры, а затем продолжает размножаться, подобно червю.

Можно предположить, что данные атаки локальны и не затронут отдельно взятый сервер. Но можно взглянуть на статистику сервера, который предоставляет услуги хостинга, конкретнее – на программу fail2ban. За период 2017-03-05 - 2017-03-12 было заблокировано 49 ip-адресов, которые многократно пытались провести подключение по ssh, доводя число до 19000 попыток от одного ip-адреса. Всего же за неделю было совершено 80 тысяч попыток подключиться.

Эксплойты. Распространение вредоносного ПОпосредством уязвимостей в операционных системах и программных продуктах. Данный способ распространения не подразумевает участия пользователя в процессе заражения системы, все уязвимые системы подвержены атаке. Уязвимости так же можно подразделить на известные сообществу, и, напротив, еще не раскрытые широким массам. Большая опасность таится именно во втором типе уязвимостей.

В качестве примера распространения вредоносного ПО посредством уязвимостей в программных продуктах рассмотрим нашумевшую атаку вируса WannaCry. Атака происходила без вмешательства пользователей: на атакованных машинах не было обнаружено скачиваний вредоносных файлов или писем, содержащих таковой. Атака происходила по следующей схеме:

1. были найдены организации и пользователи, использующие устройства, уязвимые для использования эксплоита EthernalBlue;
2. создана атакующая программа;

3. вредоносный код доставлялся до уязвимых машин с помощью эксплоита;
4. вирус заражает компьютер, создавая службу от имени системы;
5. производится поиск уязвимых устройств в локальной сети и их последующее заражение;
6. уже закрепившись в системе, вирус запрещает загрузку в режиме восстановления и удаляет сохраненные копии состояния системы;
7. шифрует файлы на зараженных машинах.

Данная вредоносная программа имеет функционал, присущий вирусам-червям, а это в свою очередь означает, что она будет распространяться по сети. Для этого она использует уязвимость EternalBlue (MS17-010), чтобы распространиться на все компьютеры, где эта уязвимость не закрыта. Немаловажный факт, червь ищет не только компьютеры в той же локальной сети зараженного компьютера, но также сканирует публичные IP-адреса в Интернете. Все эти действия выполняются службой, которую вредоносная программа устанавливает после своего запуска. После того как служба была установлена и запущена, WannaCry создает два потока для распространения себя на другие системы.

Распространившись на ограниченное количество машин, подключенных к интернету, WannaCry может распространиться по глобальной сети. В связи с тем, что первая версия вредоносной программы была снабжена так называемым killswitch (функция, останавливающая заражение), активируемый при активном сайте по определенному домену, заражение удалось остановить, но полностью избежать распространения удалось только после повсеместной установки защиты.

Подобным образом распространялся вредоносный агент NonPetya, и последствия от его проникновения не были менее разрушительными.

Мы же остановимся на фишинге ввиду простоты данного способа и в то же время разрушительной возможности. Это метод атак, абсолютно отличающийся от второго. Методы воздействия злоумышленников, использующих фишинг, находятся в области практической психологии и относятся к социальной инженерии. Играя на эмоциях, чувствах, страхах и рефлексах людей злоумышленники получают доступ к интересующей их информации. Все эти методы используются злоумышленниками при создании фишинговых почтовых сообщений и фальшивых веб-страниц.

Классический пример фишинговой атаки – почтовые письма, либо содержащие вредоносный файл, либо ведущие на фальшивые страницы авторизации, что позволить злоумышленнику завладеть искомым паролем и существенно упростить задачу проникновения в корпоративную систему, либо добычи информации.

Подобные письма зачастую воспринимаются как легитимные, потому что люди, на которые направленны такие атаки, как правило работают с большим количеством документов каждый день и такие письма их ничуть не смущают.

Помимо вредоносной ссылки, злоумышленники могут использовать уязвимости в редакторах документов и недостаточной защищенности системы. Например, не так давно пользовались популярностью атаки, использующие вредоносные макросы в документах, далее устанавливающие вредоносные агенты в систему. Нередки случаи, когда в злоумышленники проникали в систему или же получали доступ к чувствительным данным именно таким образом

В последнее время все чаще появляются новости и распространении программ-вымогателей. Этот вид вредоносной программы заражает компьютеры путем шифрования файлов и просит выкуп, чтобы восстановить зашифрованные файлы. Злоумышленники посылают письма на большое количество адресов электронной почты (массовая атака при помощи электронной почты) для того, чтобы заразить как можно больше машин, насколько это возможно. Они, как правило, используют методы социальной инженерии, написав тему и текст, не вызывающие подозрения у получателя, чтобы обмануть пользователей и заставить их скачать файл.

После открытия скачанного документа, который может иметь различные расширения (“.exe”, “.doc”, “.xls”, “.js”), вредоносная программа исполняется и шифрует данные различными алгоритмами, как правило используются RSA-2048 и AES-128. Затем пользователь получает запрос с просьбой заплатить за расшифровку. Но по статистике зачастую данные вирусы оказываются не шифровальщиками, а, так называемыми, «вайперами», то есть шифруют без возможности расшифровки.

В нашем распоряжении имеется исходный код вредоносного макроса, написанный на языке VBA. Попробуем проанализировать принцип работы.

Обычно вредоносный код добавляется в конец файла со следующими метаданными: размер вредоносного кода и контрольная сумма. Давайте взглянем на фрагменты кода, где исполняемый файл проходит подготовку для запуска:

Для начала происходит загрузка необходимых данных методом MSXML2.ServerXMLHTTP, далее происходит расшифровка данных и приведение их к готовности.

Путь для сохранения вредоносного кода обфусцирован. После деобфускации можно узнать, что значение переменной места сохранения var_Path1=”appdata\Microsoft\Word”

```
var_Path1 = Environ(Chr(97) & Chr(112) & Chr(112) & Chr(100) & Chr(97) & Chr(116) & Chr(97)) & Chr(92) & Chr(77) & Chr(105) & Chr(99) & Chr(114) & Chr(111) & Chr(115) & Chr(111) & Chr(102) & Chr(116) & Chr(92) & Chr(87) & Chr(111) & Chr(114) & Chr(100)
```

Вслучаееслипутьvar_Path1 несуществует, скриптбудетиспользоватьпросто “appdata”:

```
If Not var_Object1.FolderExists(var_Path1) Then
    var_Path1 = Environ(Chr(97) & Chr(112) & Chr(112) & Chr(100) & Chr(97) &Chr(116) & Chr(97))
  End If
  Set var_Object1 = Nothing
  Dim fh_File2
  fh_File2 = FreeFile
```

После этого происходит создание файла под названием “wfletxavb.exe” и его последующее исполнение:

```
var_Filename1 = var_Path1 & "\" & Chr(119) & Chr(102) & Chr(108) & Chr(101) & Chr(116) & Chr(120) &  Chr(97) & Chr(118) & Chr(98) & Chr(46) & Chr(101) & Chr(120) & Chr(101)
Open (var_Filename1) For Binary As #fh_File2
  Put #fh_File2, 1, var_BinaryData1
  Close #fh_File2
Erase var_BinaryData1
Set var_Object2 = CreateObject("WScript.Shell")
  var_Object2.Exec var_Filename1
  Exit Sub
ErrorCondition1:
  Close #fh_File1
  Close #fh_File2
ActiveDocument.Save
End Sub
```

Данный скрипт может быть скачен откуда угодно и запущен, если пользователь разрешит исполнение макросов. Это действительно опасное явление ввиду различных методов написания кода, который может быть обфусцирован до совершенно нечитаемого вида и вследствие не быть обнаруженным.

Для обеспечения достаточного уровня защиты системы необходимо уделять пристальное внимание любым файлам, которые загружены из сети, и запускать их в безопасном режиме либо в так называемой песочнице. Если же была обнаружена попытка создания файла от процесса, находящегося под наблюдением, то необходимо прервать данный процесс и запретить его запуск. Так же полезным будет произвести инструктаж среди сотрудников компании с целью предотвратить подробные атаки.

СПИСОК ЛИТЕРАТУРЫ

1. Ботнет Mirai [Доклад] -https://www.rsaconference.com/writable/presentations/file_upload/hta-w10-mirai-and-iot-botnet-analysis.pdf
2. Брутфорс [Электронный ресурс] - https://sfztn.com/security/brutfors-podbor-parolya-pereborom
3. Анализ вредоносного макроса [Статья] - https://spreadsecurity.github.io/2016/08/14/macro-malware-analysis.html

УДК 007

АВТОМОБИЛЬНЫЙ КЛАСТЕР САНКТ-ПЕТЕРБУРГА

Поляков Дмитрий Сергеевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, Большая Морская ул., 67
e-mail: polyakovdmitry1988@gmail.com

Аннотация. Работа посвящена рассмотрению информационно-вычислительной системы автомобиля, способствующей безопасности и созданию экологичной среды в городе. Главное внимание уделено структуре ИВС и ее описанию. Подробно рассказано о функциях автомобиля и их эффективности. Длянаглядностиработыэтихсистемиспользованыиллюстрации.

Ключевые слова: *умный автомобиль; автомобильный кластер; информационно-вычислительная система.*

CAR CLUSTER SANKT PETERSBURG

Polyakov Dmitry
St. Petersburg state University of Aerospace Instrumentation
Russia, St. Petersburg, Bolshaya Morskaya str., 67
e-mail: polyakovdmitry1988@gmail.com

Abstract. The work is devoted to the consideration of an information and computing system for the automobile that promotes security and the creation of a green environment in the city. The main focus is on

the structure of the information and computing system and its description. There are a detailed description of the vehicle's functions and their effectiveness. For clarity, the operations of these systems are illustrated.

Keywords: *smart car; cars cluster; information-computing system.*

Тема обеспечения безопасности автомобиля, участников движения и окружающих актуальна с момента создания первого автомобиля и будет оставаться актуальной до тех пор, пока существуют автомобили.

Разработка нового автомобиля, оснащенного новейшими технологиями и информационно-вычислительными системами, способными помочь водителю ориентироваться в сложной городской среде (помочь ему в восприятии зрительной информации о ситуации впереди, позади, справа и слева от автомобиля и в принятии оптимального решения, помочь ему распознать объекты, которые могут появиться с разных сторон, помочь оценить состояние дороги, помочь в восприятии информации о дорожных знаках) – основная задача создателей автомобилей.

Еще одна немаловажная задача стоит перед производителями автомобилей — это создание экологичного автомобиля.

Таким образом, цель автомобильного кластера – создание автомобиля, удовлетворяющего понятию «Умный город».

Описание проекта.

Сначала в своем реферате я рассмотрел принцип работы ИВС автомобиля. Размышляя о том, каким должен быть автомобиль будущего, я решил, что он должен быть обладателем всех самых инновационных и современных функций, какие только можно вообразить, а также положительно зарекомендовавших себя функций, пользующихся на рынке спросом.

В связи с этим, я решил использовать в автомобиле следующие функции: – ESP – Система предотвращения столкновений – Head-Up Display – Автопарковка – Умные фары – Подушка безопасности, останавливающая машину до аварии – Работа автомобиля от аккумуляторов – Кузовные панели, накапливающие энергию – Система мониторинга водителя. Для работы всех этих функций в автомобиле требуется сложная вычислительная система с большим количеством датчиков, приборов, сенсоров, исполнительных устройств и управляющих блоков. Автомобиль, включающий в себя все вышеперечисленные функции и технологии, будет соответствовать концепции «Умного города», так как все они направлены на обеспечение безопасности водителя и пешеходов, а также экологию города.

Применение данных систем приведет к минимуму количество ДТП, снизит информационную нагрузку водителя, улучшит видимость водителю, уменьшит загрязнение окружающей среды.

Автомобильный кластер является одной из ведущих отраслей в Санкт-Петербурге, и от эффективности ее работы зависит эффективность остальных сфер.

Автомобильный кластер СПБ является неотъемлемым участником концепции «Умный город», и всеми своими действиями способствует реализации ее концепции, создавая автомобили с применением инновационных технологий, которые призваны обеспечить безопасность и экологичность в городе.

СПИСОК ЛИТЕРАТУРЫ

1. Игнатьев М.Б. Кибернетическая картина мира. — СПб.: Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП), 2010. — 416 с.
2. Официальный сайт Администрации Санкт-Петербурга // Автомобильный кластер. URL: http://gov.spb.ru/gov/otrasl/c_industrial/avtomobilnyj-klaster/
3. Programmable Automotive Headlights // The ILIM laboratory at the Robotics Institute of Carnegie Mellon University. URL: http://www.cs.cmu.edu/~ILIM/projects/IL/smartHeadlight.
4. Head-Up Display // Wikipedia. URL: https://ru.wikipedia.org/wiki/Индикатор_на_лобовом_стекле 5) Autoshcool.ru // Volvo накапливаетэнергиюкузовом. URL: https://www.autoshcool.ru/5347-volvo-nakaplivaet-energiyu-kuzovom.html
5. Электронный контроль устойчивости // Wikipedia. URL: https://ru.wikipedia.org/wiki/Электронный_контроль_устойчивости
6. Автомобили на дорогах будущего // Geektimes. URL: https://geektimes.ru/company/mailru/blog/277942/ 8) Особенности и детали Volvo XC60 // Quto.ru. URL: https://quto.ru/Volvo/XC60/lf/suv5d/features/10959/
7. Электромобиль // Wikipedia. URL: https://ru.wikipedia.org/wiki/Электромобиль

УДК 656, 007; 004.81, 614.8; 007; 51-7, 351; 351.81; 351.78

ИСПОЛЬЗОВАНИЕ МЕТОДА ПОРТЕБИТЕЛЬСКОГО КОНТРОЛЯ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ

Селиверстов Ярослав Александрович, Селиверстов Святослав Александрович
Институт проблем транспорта им. Н.С. Соломенко Российской академии наук
Россия, Санкт-Петербург, 12 линия В.О., 13
e-mails: seliverstov-yr@mail.ru, seliverstov_s_a@mail.ru

Аннотация. Разрабатывается метод потребительского контроля применительно к системам транспортной безопасности и дается его формальное описание. Разрешается проблема профилактики причин возникновения дорожно-транспортных происшествий посредством перехода к

персонифицированному рекомендательному управлению потребительским поведением водителей. Даются рекомендации по дальнейшему использованию метода.

Ключевые слова: *интеллектуальные системы транспортной безопасности; умная городская логистика; системы персонального рекомендательного управления; транспортно-логистический мониторинг; интеллектуальный анализ городских данных; системы профилактики дорожно-транспортных происшествий.*

USE OF CONSUMER CONTROL IN INTELLIGENT ROAD SAFETY SYSTEMS

Seliverstov Yaroslav, Seliverstov Svyatoslav
Solomenko Institute of Transport Problems of the Russian academy of sciences
Russia, St. Petersburg, 12-th Line VO, 13
e-mails: seliverstov-yr@mail.ru, seliverstov_s_a@mail.ru

Abstract. A method of consumer control is developed for transport safety systems and its formal description is given here. The problem of prevention of the causes of road accidents is resolved through the transition to a personified recommendatory management of consumer behavior of drivers. Recommendations are given for the further use of the method.

Keywords: *intelligent road safety systems; smart urban logistics; personal recommender systems; monitoring of logistics and socio-economic processes; data mining; accident cause prevention systems.*

Введение. Рост численности населения и уплотнительная застройка густонаселенных районов в крупных городах приводят к сокращению пропускной способности улично-дорожных сетей, росту интенсивности дорожного движения и как следствие, способствуют росту числа дорожно-транспортных происшествий (ДТП) [1]. Анализ причин возникновения ДТП в России показывает, что они остаются практически неизменными - к авариям почти всегда приводит человеческий фактор [2]. Реакция и интенсивность внимания водителя в неожиданно меняющейся дорожной обстановке зависит от его психофизического состояния. Нарушение субъективного психофизического состояния водителя в ряде случаев связано с потреблением товаров, которые в силу определенных болезней, противопоказаны данному водителю.

Работа современных интеллектуальных транспортных систем (ИТС) и автоматизированных информационно-аналитических систем [3] строится на вероятностных данных. Как правило, такие системы выполняют функцию низко-вероятностного прогноза и измерения реальной транспортной ситуации в рамках существующих показателей [4]. Они также в состоянии разглядеть результат неблагоприятных дорожно-транспортных происшествий, но оперативно распознать и своевременно упредить процессы формирования городских социально-экономических, транспортных и логистических конфликтов в границах существующего программно-алгоритмического и технологического базисов для них является недостижимым шагом.

Системы способные производить интеллектуальный анализ городских транспортно-логистических процессов и удерживать характеристики объектов управления в оптимально- и допустимо- устойчивых областях будем называть городскими анализаторами транспортно-логистической и социально-экономической мобильности населения интеллектуальными (ГАТЛОСЭМИ) [5].

Городскую потребительскую, социально-экономическую и транспортно-логистическую мобильность жителя будем называть логистической мобильностью.

Функциональное наполнение системы ГАТЛОСЭМИ опирается на аналитически выведенные в [6] *условия достоверной мобильности,* обуславливающие наличие функций идентификации, аутентификации, местоопределения и распознавания состояний подвижных и стационарных объектов городской транспортной системы (ГТС).

Зададим формальную модель ГАТЛОСЭСМИ набором функционалов, согласно (1):

$$\Phi^{\Gamma} = \left\langle \begin{matrix} \mathcal{Э}^{\Gamma};\hat{F}_N;\hat{F}_C;\hat{F}_T;\hat{F}_R; \\ \hat{F}_{\Psi}^{D};\hat{F}_A;\hat{F}_{\Xi};\hat{R};C_{\mathcal{Э}^{\Gamma}};U^{\Gamma} \end{matrix} \right\rangle_T \quad (1)$$

где $\hat{F}_N : \mathcal{Э}^{\Gamma} \to N$ - функционал идентификации элементного множества $\mathcal{Э}^{\Gamma}$, который каждому объекту из $\mathcal{Э}^{\Gamma}$ ставит в соответствие идентификатор или набор идентификаторов из множества N; $\hat{F}_C : \mathcal{Э}^{\Gamma} \times I^{\Gamma} \to CH$ - функционал характеристической параметризации элементного множества $\mathcal{Э}^{\Gamma}$, который каждому объекту из $\mathcal{Э}^{\Gamma}$ с уникальным номером из I^{Γ}, ставит в соответствие, наборы характеристик, присущих данному объекту, таких что $CH = \left\{ ch_{\pi}^{\mathcal{Э}^{\hat{C}}}, \pi = 1,\ldots,N_{\pi} \right\}$ - множество

характеристик элементов $Э^{\Gamma}$, причем $ch_{\pi}^{э_c^e}$ задается кортежем $ch_{\pi}^{э_c^e} = \langle name, \{value\} \rangle$, где name – имя $\pi - й$ характеристики, {value} – область допустимых значений, которая задается перечислением этих значений, интервалом или функционально, с помощью правил вычисления (измерения) и оценки; $\hat{F}_T : \ Э^{\Gamma} \to \left[\tau_{\text{т}}^{def} \vee (\tau_{\text{т}}; \tau_{\text{т+1}})\right]$ - временной оператор, который каждому объекту из $Э^{\Gamma}$ ставит в соответствие определенный момент или интервал времени из множества моментов или интервалов времени T, на котором задано отношение строгого порядка, т.е. $\tau_1 < \tau_2, \ldots, \tau_{\text{т}} < \tau_{\text{т+1}}$; $\tau_{\text{т}}^{def} \in T$ - определенный момент времени, а $(\tau_{\text{т}}; \tau_{\text{т+1}}) \in T$ - определенный интервал времени; $\hat{F}_A : (Э^{\Gamma}; I^{\Gamma}) \to A$ - агентное отображение, которое каждому объекту из городской системы $э_c^e \in Э^{\Gamma}$ со множеством идентификаторов $I^{э_c^e}$ ставит в соответствие агента из $a_i \in A$; $\hat{F}_{\Xi} = \left\{ \Xi_A^L; \Xi_I^L; \Xi_P^L \ldots \right\}$ - функционала интеллектуального анализа графов логистического поведения населения, реализуемый через процедуры абдуктивного Ξ_A^L и индуктивного Ξ_I^L выводов, и вероятностного анализа Ξ_P^L; $\hat{R} = OCH \cup ACH \cup FCH$ - регламентирующая область логистического поведения населения, включающая область оптимально-устойчивых OCH, допустимо-устойчивых ACH и неустойчивых значений FCH характеристик населения CH и их поведение $B_t(Э_I^{\Gamma})$; $C_{Э^{\Gamma}} = (C_A \vee C_F) \vee \wedge C_{Э^{\Gamma}}^{HSB}$ - регулирующие воздействия ГАТЛОСЭМИ, состоящие из воздействий C_A рекомендательного, C_F принудительного и $C_{Э^{\Gamma}}^{HSB}$ девиантного управлений; $U^{\Gamma} = U^{\Gamma}\left(CH_U^{Э_I^{\Gamma}}\right) = \left\{ u_{э_{ic}^e}\left(\left\{ch_{\pi}^u\right\}\right)\right\}$ - целевая функция управления логистическим поведением населения (или функция полезности), зависящая от субъективных характеристик управления $\left\{ u_{э_{ic}^e}\left(\left\{ch_{\pi}^u\right\}\right)\right\}$ каждого жителя; T - множества моментов или интервалов времени.

Тогда целевой функционал ГАТЛОСЭМИ запишем в виде (2):

$$\Phi = \lim_{\substack{B_t(Э_I^{\Gamma}) \to B_t^{\Pr ef}(Э_I^{\Gamma}) \\ C_{Э^{\Gamma}} : OCH \le (CH^{\Gamma}) \le ACH}} U^{\Gamma} = \max U^{\Gamma} = U_{\Pr ef}^{\Gamma} \qquad (2)$$

где $U_{\Pr ef}^{\Gamma}$ - функция оптимального или предпочтительного управления, максимизирующая полезность жителя.

Функция полезности принимает максимальное значение $U^{\Gamma} = \max U^{\Gamma}$, в том случае, когда характеристики индивидуального поведения лежат в области оптимально - OCH и/или допустимо - ACH устойчивых значений, а само поведение является предпочтительным $B_t^{\Pr ef}(Э_I^{\Gamma})$, т.е. не приближается к потенциально-опасным шаблонам. Функционально-операторную схему ГАТЛОСЭМИ представим на рис. 1.

Рекомендательное управление поведением населения в формальном изложении, примет следующий вид:

$$Э^{\Gamma}; B_t(Э_I^{\Gamma}); CH; \hat{F}_M; \hat{R} \exists C_{Э^{\Gamma}} = \begin{cases} OCH \le |CH_{def}| \le \overline{OCH} \to \langle \varnothing; \max U^{\Gamma} \rangle \\ \underline{ACH} \le |CH_{def}| \le \overline{ACH} \to \langle C_A; U^{\Gamma} \to \max U^{\Gamma} \rangle \\ \underline{FCH} \le |CH_{def}| \le \overline{FCH} \to \langle C_F; U^{\Gamma} \to \max U^{\Gamma} \rangle \\ \lim\limits_{B_t(Э_I^{\Gamma}) \to HSB_t(Э_I^{\Gamma})} C_{Э^{\Gamma}} = C_{Э^{\Gamma}}^{HSB} \end{cases} \qquad (3)$$

где C_A - регулирующее информационное упреждающее воздействие системы рекомендательного управления; C_F - регулирующее информационное упреждающее воздействие системы принудительного управления; $C_{Э^{\Gamma}}^{HSB}$ - регулирующее информационное воздействие, упреждающее приближение индивидуального поведения жителя к потенциально-опасному шаблону.

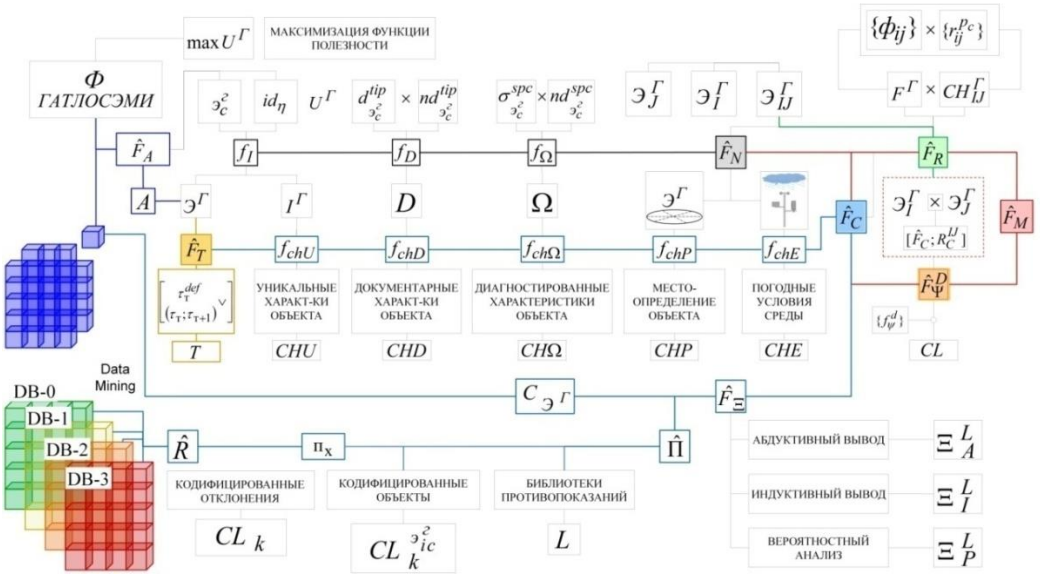


Рис. 1. Функционально-операторная схема системы ГАТЛОСЭМИ.

Под приближением индивидуального поведения жителя к потенциально-опасному шаблону будем понимать наличие в динамическом графе логистического поведения жителя потенциально опасных шаблонов из $LPDP$, согласно (4):

$$\Gamma^{date}_{\mathfrak{э}^{\mathfrak{e}}_{ic}}\left(V_{\hat{F}_C};T\right)\cap LPDP \rightarrow \begin{cases} = \varnothing, B_t\left(\mathfrak{э}^{\mathfrak{e}}_{i,c}\right) \nrightarrow HSB_t\left(\mathfrak{э}^{\mathfrak{e}}_{i,c}\right) \\ \neq \varnothing, B_t\left(\mathfrak{э}^{\mathfrak{e}}_{i,c}\right) \rightarrow HSB_t\left(\mathfrak{э}^{\mathfrak{e}}_{i,c}\right) \end{cases} \quad (4)$$

где $\Gamma^{date}_{\mathfrak{э}^{\mathfrak{e}}_{ic}}\left(V_{\hat{F}_C};T\right)$, $B_t\left(\mathfrak{э}^{\mathfrak{e}}_{i,c}\right)$ - логистическое поведения жителя $\mathfrak{э}^{\mathfrak{e}}_{ic}$; $LPDP$ - кодифицированная библиотека потенциально-опасных шаблонов логистической деятельности городского населения, где $HSB_t\left(\mathfrak{Э}^{\Gamma}_{I}\right)$- потенциально-опасное поведение, которое может привести к вхождению характеристик индивидуального поведения жителя в область неустойчивых значений.

Представленная модель рекомендательного управления индивидуальным поведением жителя реализует функцию режима профилактики возникновения широкого класса потенциально-опасных ситуаций в городской системе, в том числе с выявлением причин девиантного поведения.

Упрощенно работа ГАТЛОСЭМИ в режиме информационного упреждения потенциально-опасного шаблона поведения городского жителя представлена на рис. 2.

На рис. 2 представлена ситуация, когда городской житель, имеет нестабильную стенокардию (I20.0 по МКБ) и хронический бронхит неуточненный (J42 по МКБ). Библиотека товарных противопоказаний для этого жителя имеет вид: LGC (МКБ-10 ОКП) = ОКП 919316 (Табак соусированный и ароматизированный); а библиотека противопоказанных видов потребительской деятельности для него имеет вид: LNC (МКБ-10 LHN) =«употребление табака». В момент совершения покупки ему и продавцу приходит первое информационное уведомление, информирующее о противопоказаниях. В случае, если пользователь, имеющий девиантное поведение нулевого класса, проигнорирует первое информационное упреждение, то ему будет присвоен первый класс девиантного поведения.

В случае если городской житель продолжит продвижение по потенциально-опасному шаблону и приступит к «употребление табака», ему приходит второе информационное уведомление. В том случае, если пользователь проигнорирует второе информационные упреждения, то ему присвоен второй класс девиантного поведения.

В случае если пользователь после курения кальяна попытается приступить к управлению транспортным средством, ему будет направлено третье информационное упреждение. В том случае, если пользователь проигнорирует третье информационные упреждения, то ему будет также присвоен второй класс девиантного поведения.

В случае если пользователь совершит административное правонарушение, реализовав потенциально опасный шаблон, ему будет присвоен третий класс девиантного поведения.

В случае, если пользователь совершит уголовное правонарушение, реализовав потенциально опасный шаблон, ему будет присвоен четвертый класс девиантного поведения.

Данный пример наглядно раскрывает суть метода потребительского контроля в режиме информационного персонального упреждения городского жителя.

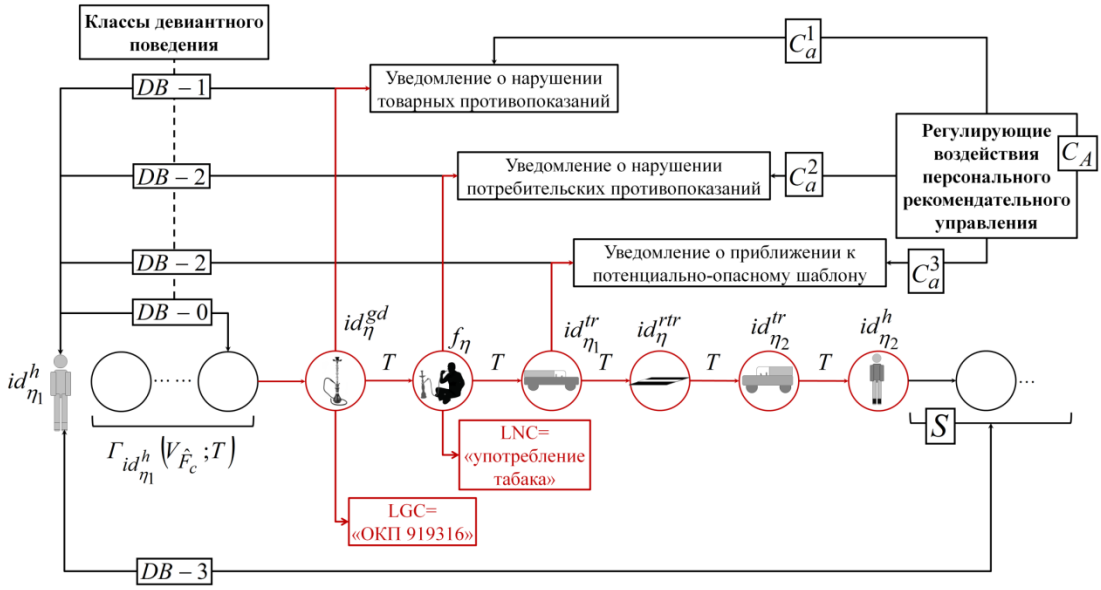


Рис.2. Выдача регулирующих воздействий рекомендательного управления пользователю.

Диагностика девиантной социально-экономической и потребительской деятельностей с кодификацией причин возникновения неблагоприятных социальных исходов и стилей поведения городского населения в режиме реального времени способначастично разрешить проблему профилактики причин возникновения ДТП посредством информационного упреждения.

Последнее открывает дорогу к совершенствованию существующих технологий анализа логистического поведения жителей и ведет к построению нового классаИТС [8, 9].

Работа выполнена при поддержке РФФИ № 16-31-00306 в рамках инициативного научного проекта (Мой первый грант) на тему: "Построение модели интеллектуального управления городскими транспортными потоками".

СПИСОК ЛИТЕРАТУРЫ

1. Ивлиев М.И., Копылов М.О., Черемисина Н.В. Экономико-статистический анализ дорожно-транспортных происшествий в России // Социально-экономические явления и процессы. 2013. № 10 (56). С. 63-66.
2. Красненкова С.А., Щелкушкина Е.А. Некоторые криминологические и индивидуально-психологические характеристики лиц, совершивших дорожно-транспортные преступления в состоянии алкогольного опьянения //Прикладная юридическая психология. 2015. № 3. С. 57-66.
3. Малыгин И.Г., Сильников М.В. Интеллектуальные системы транспортной безопасности // Проблемы управления рисками в техносфере. 2014. № 1 (29). С. 1-13.
4. Селиверстов С. А., Селиверстов Я.А. О разработке показателей анализа оценки транспортной составляющей в структуре городского квартала // Вестник транспорта Поволжья. 2015. № 4 (52). С. 55-69.
5. Каримов Т.Н., Симонова Л.А. Интеллектуальная система поддержки принятия решения для оперативного управления транспортными потоками // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2011. Т. 1. № 115. С. 37-41.
6. Селиверстов Я.А., Селиверстов С.А. Использование систем класса ГАТЛОСЭМИ для упреждения причин возникновения ДТП и неблагоприятных социальных исходов в «умном городе» // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2016. № 1 (236). С. 65-81.
7. Селиверстов Я.А., Стариченков А.Л. Построение моделей управления городскими транспортными потоками в условиях неопределенности внешней информационной среды // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2014. №6 (210). С. 81-94.
8. Zhang Xiong, Hao Sheng, WenGe Rong, Dave E. Cooper Intelligent transportation systems for smart cities: a progress review // Science China Information Sciences. 2012. Vol. 55. Iss. 12. Pp. 2908–2914.
9. Селиверстов Я.А., Селиверстов С.А. Разработка модели городского анализатора данных для интеллектуальной транспортной системы «умного города» //Транспорт: наука, техника, управление. 2016. № 12. С. 3-23.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

УДК 629.12.001.2

ПРОБЛЕМЫ СОЗДАНИЯ ИТ УПРАВЛЕНИЯ БОРЬБОЙ ЗА ЖИВУЧЕСТЬ ОМТ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ И ПЕРСПЕКТИВНЫЕ ПУТИ ИХ РЕШЕНИЯ

Алексеев Анатолий Владимирович[1], Соловьев Сергей Николаевич[2], Сус Герман Николаевич[3], Туркин Игорь Иванович[1], Москаленко Василий Александрович[2], Мусатенко Роман Иванович[2]
[1]Санкт-Петербургский государственный морской технический университет
Россия, Санкт-Петербург, ул. Лоцманская, 3
e-mails:17151@bk.ru,iitg@ya.ru
[2]Военный учебно-научный центр ВМФ «Военно-морская академия им. Н.Г. Кузнецова»
Россия, Санкт-Петербург, Ушаковская набережная, 17/1
e-mails: solserjnic@rambler.ru, vasmoskalenko@mail.ru, rus-euro-roman@yandex.ru
[3] АО «Концерн «Научно-производственное объединение «Аврора»
Россия, Санкт-Петербург, ул. Карбышева, 15
e-mail: otd614@avromail.ru

Аннотация. Рассмотрены специфика проблем создания корабельных и судовых автоматизированных комплексов. Систематизированы научно-технические и организационные перспективные пути решения проблем создания информационно-аналитических и интеллектуальных технологий автоматизации процессов борьбы за живучесть корабля, судна в информационно защищенном исполнении в обеспечение их конкурентной способности и перспективности развития.

Ключевые слова: *интеграция; интеллектуальные технологии; автоматизация процессов; борьба за живучесть корабля, судна; оптимизация системных решений.*

THE PROBLEM OF CREATING AN IT MANAGEMENT STRUGGLE FOR SURVIVABILITY OF OMT IN A SECURE EXECUTION AND PROMISING WAYS OF THEIR SOLUTION

Alekseev Anatoly[1], Solovyov Sergei[2], Boronenkov Ivan[3], Turkin Igor[1], Moskalenko Vasily[2], Musatenko Roman[2]
[1]St. Petersburg state marine technical University
Russia, St. Petersburg, Pilot str., 3
e-mails: 17151@bk.ru, iitg@ya.ru
[2] Military educational scientific center of Navy "Naval Academy. N.G. Kuznetsova"
Russia, St. Petersburg, Ushakovskaya embankment, 17/1
e-mails: solserjnic@rambler.ru, vasmoskalenko@mail.ru, rus-euro-roman@yandex.ru
[3] JSC "Concern "research-and-production Association "Aurora"
Russia, St. Petersburg, Karbysheva str., 15
e-mail: otd614@avromail.ru.

Abstract. Discusses the specific problems of the ship and ship systems. Systematized scientific-technical and organizational perspective ways of decision of problems of creation of information-analytical and intelligent technologies of automation of processes of struggle for survivability of the ship, ship information and secure execution in ensuring their competitiveness and prospects of development.

Keywords: *integration; intelligent technologies; automation processes; the struggle for the survival of the ship, vessel; optimization of system solutions.*

Среди приоритетных и ключевых проблем создания информационных технологий (ИТ) управления борьбой за живучесть объектов морской техники (ОМТ) по-прежнему определяющее место занимают ИТ автоматизации процессов борьбы за живучесть корабля, судна (ТАП БЖКС). В сочетании с ИТ математического моделирования и ИТ исследования сложных управляющих систем и процессов ТАП БЖКС традиционно являются базовыми для построения большинства современных автоматизированных корабельных комплексов и систем.

Перспективы развития ТАП БЖКС обеспечиваются сегодня комплексом актуальных научных исследований и исследовательского проектирования в областях: развития методологических и

методических основ системного (комплексного, гибридного) моделирования на основе междисциплинарных исследований и интеграции неокибернетики и общей теории систем, включая актуальные сегодня подсистемы информационной безопасности; комплексной автоматизации и интеллектуализации методов и инструментальных средств системного моделирования сложных объектов и процессов в реальном масштабе времени и в защищенном исполнении; разработки комбинированных методов, алгоритмов и методик системного моделирования и прогнозирования сложных объектов и процессов в кризисных (аварийных, нештатных, катастрофических) ситуациях, включая информационные инциденты различных видов от ошибок операторов в связи с недостаточным уровнем их подготовки (знаний, умений, владения навыками, опыта), недостаточной ответственности (халатности в исполнении регламентов, отсутствия творческой активности, разумной инициативы) до злоупотребления должностными полномочиями (нелояльности, немотивированности, меркантильности, коррумпированности и т.п.).

Уже сегодня результаты развития ТАП БЖКС все больше проявляются в разработках и повсеместном внедрение интегрированных самоорганизующихся (распределенных, полимодельных, робототехнических) комплексов. А также используемых в них комбинированных методов, алгоритмов, методик, соответствующих когнитивных технологий автоматизации моделирования сложных процессов и систем в динамических средах, в том числе повышенной агрессивности.

Специфика, критичность морской среды, техногенной среды ОМТ, особенности взаимодействия и противоборства в этих средах требуют соответствующего профессионального научно-технического анализа, синтеза, оптимизации как отдельных технических, так и системных решений в целом. Причем, критичность безошибочности, рациональности и оптимальности системных проектных решений является в условиях резкого наращивания сложности ОМТ проблемой первой значимости.

Особым ресурсом в этой связи является интеграция профессиональных знаний специалистов всех уровней от высшей школы до разработчиков современных корабельных и судовых систем автоматизации. В систематизированном виде приоритетными направлениями развития ТАП БЖКС, по нашему мнению, сегодня являются: интеллектуализация каналов контроля технического состояния ОМТ, число которых сегодня превышает 2000 и требует практически полного покрытия контурами автоматического управления; информационно-аналитическая и интеллектуальная поддержка решений лиц, принимающих решения (ЛПР), их обосновывающих (ЛОР) и исполняющих (ЛИР), прежде всего, с целью алгоритмической нейтрализации негативного влияния их субъективных («человеческих») факторов. В этой связи особую значимость и перспективность приобретает создание автоматизированных средств и систем в информационно защищенном исполнении (АСЗИ); оптимизация процессов и технологий мониторинга, прогнозирования и управления, включая минимизацию избыточности интерфейсных (экранных) форм, максимизацию охвата решаемых задач контурами автоматического управления в информационно защищенном исполнении; системная эрготехническая оптимизация комплексных технологических решений с целью минимизации психофизиологической нагрузки на ЛПР, ЛОР и ЛИР на всех этапах службы экипажа, включая стрессовые перегрузки в процессе локализации аварийных ситуаций, аварий (ЛА) и БЖКС; мониторинг и прогнозирование системных (сводных, агрегированных) показателей качества функционирования систем диагностики и управления ОМТ с целью гарантированного решения АСЗИ задач обеспечения безопасной эксплуатации (ОБЭ) технических средств, их систем и оружия (ТССО); тренажерная отработка и совершенствование алгоритмов оптимизации принятия решений в АСЗИ, регламентов обслуживания и использования ТССО как при ОБЭ, ЛА, так и при БЖКС; внедрение в АСЗИ подсистем объективной оценки компетенций и адекватности персонала на всех стадиях их подготовки, переподготовки, а также непосредственно при эксплуатации АСЗИ; совершенствование средств и методов верификации внедряемых в АСЗИ программных комплексов на всех стадиях их жизненного цикла, создания и эксплуатации ТССО; оптимизация концептуальных решений и комплекса требований к ОМТ, средств и методов их полимодельной верификации и валидации, а также технологий их реализации в АСЗИ; концептуальное и проектное обоснование и аттестация конкурентной способности ТАП БЖКС и перспектив их развития с использованием современных методов квалиметрического обеспечения.

Среди организационно-технических задач и направлений развития ИТ ОМТ и, в первую очередь, ТАП БЖКС наиболее актуальными, по мнению авторов, следует считать: проведение межведомственных конференций, семинаров, мастер-классов, тренингов, вебинаров, круглых столов по систематизации и популяризации лучших практик и ТАП БЖКС; проведение партнерской (добровольной, открытой) ранговой (по достигаемому уровню качества в дополнение к подтверждению соответствия заданным требованиям) сертификации средств и систем ОМТ в обеспечение их конкурентной способности и перспективности развития, проведение открытых конкурсов на лучшее технологическое решение, патент, доклад, публикацию и ведение открытых баз данных по ним, включая результаты квалиметрических оценок качества и конкурентной способности

по национальному и мировому уровням; участие некоммерческих партнерств, экспертных советов и сообществ в независимой экспертизе и информационно-аналитической поддержке принятия решений организациями, центрами экстренной дистанционной поддержки и реагирования, ситуационными центрами и т.п.; издание открытых монографий по лучшим практикам внедрения ИТ ОМТ, ТАП БЖКС; консолидацию усилий научных школ отрасли на главных направлениях развития перспективных ИТ ОМТ и ключевых ТАП БЖКС.

В качестве средств реализации указанных задач целесообразно, по нашему мнению, рекомендовать следующие приоритетные научные направления исследований: дальнейшее совершенствование понятийного аппарата ИТ ОМТ и развитие единой методологии системной и технологической оптимизации проектных решений, в том числе по ТАП ОБЭ, ЛА и БЖКС; реализацию методов визуализации, мониторинга, контроля и прогнозирования состояния средств и систем ОМТ на основе интегрированных АСЗИ; дальнейшее развитие и разработку методов и технологий создания комплексных баз данных и знаний, в том числе по лучшим практикам АП БЖКС.

Тем самым, систематизация данных по проблеме создания ИТ управления БЖКС в защищенном исполнении позволяет определить перспективные пути решения этой актуальной проблемы, что обеспечит ускорение развития и формирование условий для создания конкурентно способных образцов отечественной морской техники и технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Соколов И.А. Основные методологические подходы к созданию автоматизированных систем управления, создаваемых для обороны страны и обеспечения безопасности государства / Оружие наследников Победы. – М.: Издательский дом «Оружие и технологии», 2015, с. 96 – 107.
2. Алексеев А.В. Концептуальные аспекты управления развитием критических объектов морской техники и морской инфраструктуры / Морские интеллектуальные технологии, 2015, № 2 (28), т. 1, с. 47 - 57.
3. Гаврилов А.Ф., Дымент А.Б., Киваев Н.М., Масленников Ю.А. Системы поддержки принятия решений в ИСБУ ПЛ – составная часть искусственного интеллекта систем управления // Системы управления и обработки информации: научн.-техн. сб. /ОАО «Концерн «НПО «Аврора», СПб., 2015. Вып. 31, с. 12 – 17.

УДК 629.12

РЕГРЕССИОННЫЙ АНАЛИЗ ДИНАМИКИ 10 ЛЕТ ХАКЕРСКИХ АТАК И ИНФОРМАЦИОННЫХ ИНЦИДЕНТОВ

Анциферов Александр Владимирович
Санкт-Петербургский государственный морской технический университет
Россия, Санкт-Петербург, ул. Лоцманская, 3
e-mail: ava1996@yandex.ru

Аннотация. Рассмотрена проблема систематизации и анализа динамики 10 лет хакерских атак и информационных инцидентов, наиболее распространенные виды хакерских атак. Приведены примеры и сравнительные оценки комплексной защиты типовых ОМТИ. Сформулированы 5 предложений по организационно-технической защите населения от информационного «разбоя».

Ключевые слова: *комплексная безопасность; хакер; взлом; защита; уязвимость.*

REGRESSION ANALYSIS OF THE DYNAMICS OF 10 YEARS OF HACKING AND INFORMATION INCIDENTS

Antsiferov Alexander
State MarineTtechnical University of St. Petersburg
Russia, St. Petersburg, Lotsmanskaya str., 3
e-mail: ava1996@yandex.ru

Abstract. The problem of systematization and analysis of the dynamics of 10 years of hacker attacks and information incidents, the most common types of hacker attacks. The examples and comparative assessment of integrated protection of the model of OMTI. Formulated 5 proposals for organizational and technical protection of the population from the information of "robbery".

Keywords: *comprehensive security; hacker; hacking; security; vulnerability.*

Среди проблем повышения качества и эффективности современных систем автоматизации и обеспечения комплексной безопасности в том числе объектов морской техники и инфраструктуры (ОМТИ) определенное значение имеет проблемный вопрос систематизации и анализа динамики, например, за 10 лет хакерских атак и информационных инцидентов, а также рассмотрения технологий наиболее распространенных видов хакерских атак и защиты от них [1 - 4].

«Hack» — по-английски когда-то обозначало массу понятий с общим значением «что-то резко обрывать». Были еще и другие варианты. Позже термин «hacking» стал толковаться как компьютерное хулиганство [1].

«Хакер» — это взломщик информационных ресурсов разного вида, включая сайты и сервера. Человек, использующий свое мастерство для разных, иногда неблаговидных целей. Сейчас это для одних — индустрия, а для других — стиль жизни. Вторые предпочитают называть себя не «хакерами», а «хэкерами». Это - целое международное сообщество. Они взламывают сети из «спортивного» интереса и, уходя, зачастую «латают дыры» [1, 2].

«Чистые» хакеры не только не причиняют вреда, но и приносят пользу, указывая на слабые места в системе защиты информационных систем. И часто делают это бескорыстно. Иной раз и по просьбе самого владельца сети, желающего узнать эти самые «слабые» места.

В истории Интернета самые известные хакерские атаки постоянно публикуются в сетях, но, как и в айсберге, большая часть событий и технологий остаются невидимыми.

Кевин Митник [2], наверное, самый известный в мире американский хакер. Во многом - благодаря склонности к эксцентричному поведению, которого от него и ожидала праздная публика.

Во время своего ареста в 1995 году Митник безапелляционно заявил, что ему достаточно посвистеть в трубку уличного телефона-автомата, чтобы (!) развязать ядерную войну.

Будучи студентом, с компьютера TRS-80 Митник проник в глобальную сеть ARPANet, предшественницу Internet, и через компьютер Лос-Анджелесского университета «добрался» до серверов Министерства обороны США. Взлом был зафиксирован. Юного киберпреступника довольно быстро нашли. В итоге он отбыл полгода в исправительном центре для молодежи. Любопытный факт: он проделал это на компьютере с частотой процессора меньше 2 МГц.

Американец Джонатан Джеймс — первый несовершеннолетний хакер, осужденный в США за киберпреступления. Как утверждало обвинение, в 15-летнем возрасте в 1999 году он взломал компьютерную систему собственной школы, сеть телекоммуникационной компании Bell South, а затем проник на сервер Министерства обороны США [3].

Здесь он перехватил более трех тысяч электронных писем сотрудников госучреждений, взломал сервер НАСА и похитил программное обеспечение, предназначенное для управления системами жизнеобеспечения на Международной космической станции.

Кевин Поулсен - еще один бывший хакер, сменивший род занятий, как и Митник, на более безопасный [4]. В восьмидесятых годах Поулсен специализировался на взломе телефонных линий и с легкостью манипулировал номерами и каналами разных операторов.

Впервые Поулсен стал известен под псевдонимом Dark Dante в 1993 году после взлома системы управления телефонными линиями Лос-Анджелесской радиостанции KIIS-FM.

В результате искусной блокировки линий он стал победителем нескольких конкурсов и как 102-й дозвонившийся «выиграл» автомобиль Porsche 944 S2.

Выводы.С учетом данных регрессионного анализа по динамике информационных инцидентов только за 10 последних лет хакерских атак и других информационных инцидентов можно утверждать:

1. Актуальность систематизации данных по информационным инцидентам возрастает как в связи с ростом их числа, так и с еще более заметным возрастанием сложности информационных инцидентов, их «изощренности» и масштабом роста наносимого при этом ущерба.

2. При этом анализе с учетом специфики процессов не должно допускаться дилетантства, так как возникающие при этом «страшилки» только поднимают интерес, особенно, у молодежи к «романтике удивлять мир». Это неизбежно приводит к росту «армии экспериментаторов», для нейтрализации которой может просто не хватать ресурсов.

3. Поэтому заслуживает внимание такое направление информационно-психологического противоборства информационно зловредным действиям «любителей» как профессиональная (без паники и пустых слов) оценка инцидентов и популяризация «информационной гигиены населения».

4. В сочетании с активной правоприменительной практикой и должным реагированием правоохранительных структур на каждый информационный инцидент это позволит по существу управлять далеко не простыми, но социально опасными угрозами и ситуациями.

5. Прежде всего, информационно защищать общественность (прежде всего, самые мало защищенные слои населения – пенсионеров, граждан с гуманитарным образованием и объективно далеких от «технологий защиты») от массовых «тараканьих бегов» по «открытым пространствам».

В том числе от «информационного разбоя» в форме массовых социоинженеринговых взломов личных счетов граждан, телефонных «блокировок» счетов руками их владельцев и т.п., на которые сегодня полиция практически не реагирует, хотя имеет для этого все необходимые ресурсы. Но в силу своих специфических свойств «оборотней» эту информацию, получая от пострадавших граждан «из рук не выпускают» и, имеются основания утверждать, «активно используют». Благо спрос на «безответную» защиту возрастает лавинообразно. Может, это тоже «бизнес»?

СПИСОК ЛИТЕРАТУРЫ

1. Научный журнал «Молодой учёный».
2. Журнал «Хакер».
3. https://ria.ru/spravka/20130808/955191308.htm.
4. http://m.diletant.media/articles/26011961

УДК 629.12

АНАЛИЗ УЯЗВИМОСТЕЙ СЕРВИСОВАВТОРИЗАЦИИ И ВОЗМОЖНОСТИ ИХ СОВЕРШЕНСТВОВАНИЯ

Бирюкова Александра Валерьевна
Санкт-Петербургский государственный морской технический университет
Россия, Санкт-Петербург, ул. Лоцманская, 3
e-mail: biryukova.aleksasha@mail.ru

Аннотация. Проведен анализ уязвимостей различных сервисов авторизации и возможности их совершенствования в настоящее время.

Ключевые слова: *мониторинг; пользователь; система программное обеспечение; тестирование.*

ANALYSIS OF VULNERABILITY OF SERVICES AUTHORIZATION AND POSSIBILITIES OF THEIR IMPROVEMENT

Biryukova Aleksandra
State MarineTtechnical University of St. Petersburg
Russia, St. Petersburg, Lotsmanskaya str., 3
e-mail: biryukova.aleksasha@mail.ru

Abstract. The analysis of vulnerabilities of various authorization services and the possibility of their improvement at the present time has been carried out.

Keywords: *monitoring; user; system software; testing.*

В настоящее время большое внимание уделяется мониторингу парольной защиты информационных ресурсов, а именно - мониторингу парольной защиты и контролю надежности пользовательских паролей. Мониторинг попыток несанкционированного доступа, предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы, специальных программных средств.

Мониторинг производительности автоматизированных систем производится по обращениям пользователей в ходе обслуживания систем и при проведении профилактических работ.

Системный аудит производится администратором информационной безопасности ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности с занесением записей в Журнал обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

Журналы обзоров безопасности должны включать несколько важных пошаговых функций.

Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему с помощью автоматического инструментария или вручную.Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы.Внесение изменений в системное программное обеспечение осуществляется с условием обязательного документирования изменений в соответствующем журнале; уведомлением каждого сотрудника, которого касается изменение; рассмотрением претензий в случае, если внесение изменений повлекло причинение вреда; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

Выводы.

1. Технологии сервисов авторизации сегодня весьма совершенны и непрерывно развиваются, что позволяет утверждать о возможности эффективной защиты данных на их основе.

2. Анализ уязвимостей сервисов авторизации показал необходимость и возможность их совершенствования в направлении упрощения интерфейсов, сокращении времени процедур, в том числе при использовании многоранговой авторизации.

СПИСОК ЛИТЕРАТУРЫ

1. https://ria.ru/spravka/20130808/955191308.htm.
2. http://m.diletant.media/articles/26011961

УДК 629.12

УЯЗВИМОСТИ, УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОЦЕНКА СТЕПЕНИ ЗАЩИЩЕННОСТИ ДАННЫХ СЕРВИСА OUTLOOK

Кармазин Жан Романович
Санкт-Петербургский государственный морской технический университет
Россия, Санкт-Петербург, ул. Лоцманская, 3
e-mail: zhan5555@yandex.ru

Аннотация. Рассмотрена проблема уязвимости, угрозы информационной безопасности и оценка степени защищенности данных сервиса Outlook, наиболее распространенные виды уязвимостей и угроз. Приведены примеры и оценки комплексной защиты Outlook. Сформулированы предложения по организационно-технической защите пользователей Outlook.

Ключевые слова: *Outlook; уязвимость; угроза информационной безопасности; защита; степень защищенности.*

VULNERABILITY, THREATS, AND ASSESSMENT OF DEFINITION OF SERVICE DATA OUTLOOK

Karmazin Zhan
St. Petersburg State Maritime Technical University
Russia, St. Petersburg, Lotsmanskaya str., 3
e-mail: zhan5555@yandex.ru

Abstract. The problem of vulnerability, threats to information security and evaluation of the degree of security of data in the Outlook service are considered, the most common types of vulnerabilities and threats. Examples and evaluations of complex Outlook protection are given. Proposals on organizational and technical protection of Outlook users are formulated.

Keywords: *Outlook; vulnerability; threat of information security; protection, degree of security.*

Известно, что вычислительная техника и практические результаты ее применения стали мощным двигателем научно-технического прогресса. Современное состояние уровня применения вычислительной техники характеризуется расширением спектра используемой информации и, как следствие, оснащение специалистов аппаратными и программными средствами, способными справиться с огромными потоками данных. Одним из средств автоматизации рабочего места является Microsoft Outlook, входящий в состав офисного пакета Microsoft Office. Данный инструмент обладает достаточно широким кругом возможностей, среди которых стоит назвать ведение базы контактов, планирование задач, коммуникации через сеть Интернет и т.д. Работа с Microsoft Outlook проста и понятна, что делает данную программу доступной для широкого круга пользователей, освобождая их от рутинной работы и автоматизируя важные процессы профессиональной деятельности.

Приложение Microsoft Outlook – мощный инструмент для организации индивидуальной и групповой работы на компьютере. Outlook представляет собой программу управления данными. Outlook может использоваться для документооборота, формирования задач и заданий группы, управления электронной почтой, планирования дел и собраний, ведения списка контактных лиц и дневника выполняемых действий.

Одной из проблем, препятствующих повышению качественного уровня и эффективности современных систем автоматизации и обеспечения информационной безопасности объектов морской техники и инфраструктуры (ОМТИ), является угроза информационной безопасности, связанная с использованием сервиса Outlook.

С учетом анализа безопасности сервиса Outlook можно утверждать, что актуальностьрешения этой проблемы заключается в том, чтоабсолютной безопасности сервиса Outlook не существует. Однако, есть множество приемов, позволяющих к ней приблизиться. Степень защиты, как правило, напрямую зависит от ценности, как хранимой на компьютере информации, так и той, к которой этот компьютер имеет доступ.

СПИСОК ЛИТЕРАТУРЫ

1. Джоан Преппернау, Джойс Кокс : Microsoft Office Outlook 2007. Шаг за шагом : Москва, Эком, 2007 :: 544 стр.
2. http://computersbooks.net/books/rukovodstvo-po-po/padvik-g/2002/files/ispolzovaniemicrosoftoutlook2002.pdf.
3. http://www.securitylab.ru/news/477828.php.

УДК 656.611

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В МОРСКОМ СЕКТОРЕ ЕВРОПЕЙСКОГО СОЮЗА

Колесникова Марина Львовна
Институт Европы РАН
Россия, г. Москва, Моховая ул., дом 11, стр. 3В
e-mail: kml2007@mail.ru

Аннотация. В работе рассматривается опыт Европейского союза по обеспечению информационной безопасности в морском секторе. Данный опыт может быть использован для разработки подходов к управлению указанной сферой в Российской Федерации.

Ключевые слова: *информационная безопасность; морская деятельность; Европейский союз.*

INFORMATION SECURITY IN THE MARITIME SECTOR OF THE EUROPEAN UNION

Kolesnikova Marina
Russia, Moscow, Mokhovaya str. 11, building 3B
e-mail: kml2007@mail.ru

Abstract. The article discusses the experience of the European Union on information security in the Maritime sector. This experience can be used to develop approaches to the management of the specified field in the Russian Federation.

Keywords: *information security; sea activity; European Union.*

Развитие функциональных видов морской деятельности связано с расширением количества вызовов и угроз, обусловленных усложнением отраслевых производственных процессов, ускорением цифровой трансформации и усовершенствованием программно-аппаратных средств. Учитывая то обстоятельство, что большая часть морских хозяйственных операций проходит в условиях постоянного воздействия агрессивной внешней среды, наличия высокой степени экологических рисков и повышенной вероятности нанесения значительного материального ущерба, обеспечение информационной безопасности является обязательным условием для эффективного осуществления морской деятельности.

В настоящее время растущий уровень кибератак оценивается как серьезная угроза для морской промышленности и судоходства [1]. О повышении активности киберпреступников говорится в отчете "Разворот и трансформация в области кибербезопасности" за 2016 г., подготовленном международной компанией PwC, которая специализируется на консалтинговой и аудиторской деятельности [2]. Расширение автоматизации морской деятельности, использование электронной навигации, автоматических идентификационных систем (АИС), а также перспективы перехода на беспилотное управление судами существенно повышают риски для судоходства от деструктивного информационного воздействия. Данная ситуация усугубляется низким уровнем информированности о кибербезопасности [3].

В 2014 г. международная компания CyberKeel (Копенгаген, Дания), специализирующаяся в области морской кибербезопасности, опубликовала доклад Maritime Cyber-Risks. В документе отмечается уязвимость морской промышленности перед широким спектром киберрисков и отсутствие необходимой защиты от этих рисков. В качестве одного из примеров в докладе приводится кибератака на иранскую судоходную линию IRISL в августе 2011 г. В результате были повреждены данные, "касающиеся тарифов, погрузки, номера груза, даты и места", компания потеряла груз и понесла существенные финансовые потери [4]. В докладе отмечается, что кибератаки оказывают негативное воздействие не только на компании, но и на национальную безопасность государств [5]. Компания CyberKeel считает, что оцифровка судовых аппаратных средств и бизнес-моделей в морской промышленности повышает значение кибербезопасности как важного условия управления морскими рисками [6].

Таким образом, необходимость обеспечения информационной безопасности в морском секторе обусловлена объективными условиями, сложившимися в результате естественного развития информационно-коммуникационных технологий (ИКТ). В этой связи целесообразно исследовать и проанализировать накопленный в данной сфере опыт мирового сообщества, отдельных государств и Европейского союза с целью его научной оценки и определения возможностей использования этого опыта в морской практике Российской Федерации.

Опыт Европейского союза

В настоящее время членами Европейского союза являются 28 государств, 23 из которых имеют выход к морю. 90% внешней торговли ЕС и 40% внутренней торговли осуществляется морским путем. Европейские судовладельцы управляют 30% мировых судов и 35% мирового тоннажа судоходства – в том числе 55% контейнерных судов и 35% танкеров, что в целом составляет около 42% стоимости мировой морской торговли. Ежегодно через порты ЕС проходят более 400 млн пассажиров. Более

20% мирового тоннажа зарегистрировано под флагом государств-членов ЕС, а более 40% мирового флота контролируется компаниями ЕС. Численность рыболовного флота ЕС в 2011 г. составила 83014 судов с валовым тоннажем 1696175 [7].

Учитывая значительные объемы морехозяйственной деятельности, Европейским союзом принимаются соответствующие меры к обеспечению информационной безопасности, в том числе для морского сектора. "Безопасность становится ключевым приоритетом, поскольку связь и информация являются ключевым фактором экономического и социального развития",... безопасность [сетей и информационных систем] выступает предпосылкой дальнейшего прогресса", говорится в одном из документов Европейского союза (2001 г.), в котором формулируются подходы к обеспечению информационной безопасности [8].

В 2004 г. Постановлением № 460/2004 Европейского парламента и Совета ЕС была учреждена организация, которая занимается вопросами информационной и сетевой безопасности Европейского союза – Агентство Европейского союза по сетевой и информационной безопасности (European Network and Information Security Agency, ENISA). В 2013 г. в соответствии с Регламентом ЕС № 526/2013 Европейского парламента и Совета от 21 мая 2013 г. ведомство было переименовано в Агентство Европейского союза по вопросам сетевой и информационной безопасности (The European Union Agency for Network and Information Security). Аббревиатура ENISA осталась без изменений. Целью создания ENISA стало "обеспечение высокого и эффективного уровня сетевой и информационной безопасности" и "развитие сетевой культуры и информационной безопасности", отвечающей потребности бесперебойного функционирования внутреннего рынка [9].

Ко времени создания ENISA Европейским союзом был разработан ряд нормативных документов, направленных на решение вопросов обеспечения безопасности в информационной сфере. В их числе следующие документы:

Директива 2002/21/ЕС Европейского парламента и Совета от 7 марта 2002 г. [10] об общей нормативной базе для сетей и услуг электронных коммуникаций (Рамочная директива), которая "устанавливает согласованные рамки регулирования услуг электронной связи, сетей электронной связи, связанных с ними объектов и связанных с ними услуг, "определяет задачи национальных регулирующих органов и устанавливает комплекс процедур для обеспечения согласованного применения нормативной базы на всей территории Сообщества";

Директива 2002/20/ЕС об авторизации электронных коммуникационных сетей и услуг (Директива об авторизации). Ее цель – совершенствование внутреннего рынка электронных коммуникационных сетей и услуг ЕС посредством гармонизации и упрощения правил и условий авторизации [11];

Директива Европейского Парламента и Совета Европейского Союза 2002/58/ЕС от 12 июля 2002 г. "в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи)" [12].

В ноябре 2005 г. Европейской комиссией разработана "Зеленая книга" (Green paper) по созданию Европейской программы защиты важнейших объектов инфраструктуры (European Programme for Critical Infrastructure Protection, EPCIP), в которой были предложены и вынесены для обсуждения заинтересованных сторон варианты EPCIP. Цель "Зеленой книги" – разработка мер по защите критической инфраструктуры от повреждений, уничтожений или нарушений в результате преднамеренных актов терроризма, стихийных бедствий, халатности, несчастных случаев, а также компьютерных хакерских атак [13]. Ранее, в 2004 г., в Сообщении "Защита критической инфраструктуры в борьбе с терроризмом" было предложено сформировать Информационную сеть предупреждения для критической инфраструктуры (CIWIN) [14].

В "Зеленой книге" сформулировано определение "критическая информационная инфраструктура" (Critical Information Infrastructure – CII). Под CII подразумеваются продукты ИКТ, которые являются критическими инфраструктурами (Critical Infrastructure – CI) или сами по себе, или выступают элементами в составе других инфраструктур (телекоммуникации, компьютеры / программное обеспечение, Интернет, спутники и т.д.). Там же формулируется понятие "защита критической информационной инфраструктуры (Critical Information Infrastructure Protection – CIIP), которое рекомендуется рассматривать как межсекторальное явление.

В 2006 г. опубликовано Сообщение Европейской комиссии, в котором излагаются "принципы, процессы и инструменты", предлагаемые для реализации EPCIP [15]. Программа EPCIP предусматривала осуществление процедур выявления и назначения критических европейских инфраструктур (ECI), а также организацию мер, содействующих выполнению EPCIP. Они включали план действий EPCIP, формирование CIWIN, ряд других мер. В целях улучшения защиты важнейших национальных инфраструктур каждому государству-члену предложено разработать национальную программу защиты критической инфраструктуры (Critical Infrastructure Protection, CIP). Такие программы нацелены на самостоятельное определение подходов каждого государства-члена Европейского союза к защите важнейших национальных инфраструктур, расположенных на его территории. Приоритетными секторами в рамках реализации Плана действий стали транспорт и энергетика.

В Сообщении Европейской Комиссии «На пути к общей политике по борьбе с киберпреступностью» 2007 г. дано определение понятия "киберпреступность" и сформулированы предложения по борьбе с данным явлением [16].

В 2008 г. была принята Директива Совета 2008 /114 / ЕС о выявлении и назначении важнейших европейских инфраструктур, а также оценке необходимости улучшения их защиты [17]. Ее реализация осуществляется в энергетическом и транспортном секторах. Как отдельное направление транспортной отрасли в опубликованном в приложении к директиве списке секторов Европейской критической инфраструктуры (European critical infrastructure – ECI) выделены океанское и каботажное судоходство, а также порты. В список ECI в энергетическом секторе включены трубопроводы и терминалы сжиженного природного газа (СПГ).

Киберугрозы признаны препятствием для создания современной информационной инфраструктуры в рамках реализации "Цифровой повестки для Европы" (Digital Agenda for Europe) [18]. Это – одна из семи инициатив принятой в 2010 г. Стратегии "Европа - 2020" – «Развитие цифровых технологий в Европе», которая направлена на использование потенциала ИКТ и обеспечение устойчивых экономических и социальных выгод от цифрового единого рынка, в том числе на развитие и применение трансъевропейских цифровых услуг.

30 марта 2009 г. Комиссия приняла Сообщение о защите критически важной информационной инфраструктуры [21], в котором основное внимание уделяется защите Европы от кибератак и киберпреступлений путем повышения готовности, безопасности и устойчивости, а также План действий, призывающий ЕНИСА играть определенную роль в поддержке государств-членов.

В декабре 2011 г. ENISA опубликовало первый в своем роде доклад, посвященный анализу аспектов информационной безопасности в морском секторе, В документе представлен базовый анализ обеспечения кибербезопасности на море и сформулированы рекомендации по устранению рисков [20]. В докладе отмечается критическая зависимость европейской экономики от морских перевозок грузов и пассажиров. В связи с этим обеспечение критической инфраструктуры морского сектора становится приоритетным направлением деятельности для Европейского союза.

Основные выводы доклада:

низкая осведомленность о морской кибербезопасности на море на всех уровнях управления морской деятельностью, включая государственные органы, портовые власти и морские компании;

недостаточная готовность к противодействию киберугрозам;

растущая зависимость от ИКТ и их усложнение, что повышает уязвимость информационной среды для кибератак;

отсутствие координации между заинтересованными сторонами на разных уровнях.

В предложенной в 2013 г. Стратегии кибербезопасности Европейского союза "Открытое, безопасное и защищенное киберпространство" [20] изложены взгляды ЕС в этой сфере и перечислены действия по защите информационной среды ЕС.

В принятой в 2014 г. Стратегии морской безопасности ЕС (The European Union Maritime Security Strategy, EUMSS) кибератаки включены в число рисков и угроз для безопасности на море как преднамеренные незаконные акты на море и в портах в отношении судов, грузов, экипажей и пассажиров, портов, портовых сооружений, критической морской и энергетической инфраструктуры [21].

Директива о безопасности сетевых и информационных систем (The NIS Directive) принята Европейским парламентом 6 июля 2016 г. и вступила в силу в августе 2016 г. Государства-члены "имеют 21 месяц для включения Директивы в свое национальное законодательство и еще 6 месяцев для выявления операторов основных услуг" [22]. В документе определяются меры, направленные на достижение высокого общего уровня безопасности сетевых и информационных систем в рамках ЕС и улучшения функционирования внутреннего рынка. Согласно Ст. 5 указанной Директивы, к 9 ноября 2018 г. государства-члены должны идентифицировать операторов основных услуг, которые включают морские транспортные компании.

Заключение. Цифровая трансформация морской деятельности требует наращивания соответствующих мер информационной безопасности в объеме, обеспечивающем необходимый и достаточный уровень защиты. Наиболее существенные вызовы и угрозы связаны с морскими отраслями, функционирование и развитие которых зависит от использования современных программно-аппаратных средств (систем), прежде всего, в морском судоходстве. В частности, к области особо уязвимых объектов можно отнести практически весь парк морских грузовых и пассажирских судов, а также средства управления, связи, навигационно-гидрографического и гидрометеорологического обеспечения.

В Доктрине информационной безопасности Российской Федерации отмечается, что широкое распространение информационно-коммуникационных технологий во всех областях деятельности повышает актуальность мер, направленных на обеспечение безопасности Российской Федерации в информационной сфере, в том числе по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления [23].

В этой связи опыт Европейского союза в сфере информационной безопасности может иметь существенное практическое значение для отраслевого развития морского транспорта и обеспечивающей его береговой инфраструктуры Российской Федерации, а также для повышения эффективности морехозяйственной деятельности в целом как составной части экономического развития нашей страны.

СПИСОКЛИТЕРАТУРЫ

1. Lars Jensen. Technology Challenges in Maritime Cyber-Resilience // Innovation Management Review. April 2015: website. URL: http://timreview.ca/sites/default/files/article_PDF/Jensen_TIMReview_April2015.pdf (дата обращения: 31.08.2017).
2. Turnaround and transformation in cybersecurity // Официальныйсайткомпании PwC: URL: http://www.pwc.ru/ru/riskassurance/publications/assets/gsiss2016-report.pdf (датаобращения: 8.09.2017).
3. Safety and Shipping Review 2015. // Allianz Global Corporate & Specialty SE: website. URL: https://www.allianz.com/v_1427190309000/media/press/document/other/Shipping-Review-2015.pdf (дата обращения: 11.09.2017).
4. Lars Jensen. Technology Challenges in Maritime Cyber-Resilience // Innovation Management Review. April 2015: website. URL: http://timreview.ca/sites/default/files/article_PDF/Jensen_TIMReview_April2015.pdf (дата обращения: 31.08.2017).
5. Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas. CyberKeel, 2014: website. URL: http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf. (дата обращения: 24.09.2017).
6. Maritime Cyber Security // CyberKeel. 2017: website. URL: https://www.cyberkeel.com/ (дата обращения: 24.09.2017).
7. Towards an EU integrated approach to global maritime security // European Commission. 2017: website. URL: http://europa.eu/rapid/press-release_IP-14-224_en.htm (дата обращения: 24.09.2017).
8. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "Network and Information Security: Proposal for A European Policy Approach". COM (2001) 298 final // EU law and publications: website. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298 (датаобращения: 24.09.2017).
9. Regulation (EC) № 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency // EU law and publications: website. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML (дата обращения: 3.09.2017).
10. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 // EU law and publications: website. URL: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0021 (дата обращения: 2.09.2017).
11. Директива Европейского парламента и Совета Европейского Союза 2002/20/ЕС от 7 марта 2002 г. об авторизации электронных коммуникационных сетей и услуг (Директива об авторизации) // ГАРАНТ: информационно-правовой портал. URL: http://base.garant.ru/70205136/ (дата обращения: 17.09.2017).
12. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) // EU law and publications: website. URL: http://ec.europa.eu/justice/data-protection/law/files/recast_20091219_en.pdf (дата обращения: 17.09.2017).
13. Green Paper on a European Programme for Critical Infrastructure Protection COM (2005) 576 final // EU law and publications: website. URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52005DC0576 (дата обращения: 15.09.2017).
14. Communication from the Commission to the Council and the European Parliament Critical Infrastructure protection in the fight against terrorism. COM (2004) 702 final // EU law and publications: website. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0702&from=en (дата обращения: 17.09.2017).
15. Communication from the Commission on a European Programme for Critical Infrastructure Protection COM (2006) 786 final // EU law and publications: website. URL: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52006DC0786 (дата обращения: 12.09.2017).
16. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions of 22 May 2007 "Towards a general policy on the fight against cyber crime" COM (2007) 267 final // EU law and publications: website. URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52007DC0267 (дата обращения: 12.09.2017).
17. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection // EU law and publications: website. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN (дата обращения: 12.09.2017).
18. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digital Agenda for Europe COM (2010) 245 final // EU law and publications: website. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2010:0245:FIN (дата обращения: 12.09.2017).
19. Analysis of cyber security aspects in the maritime sector // The European Union Agency for Network and Information Security. December 19, 2011: website. URL: https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1 (дата обращения: 12.09.2017).
20. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace // EU law and publications: website. URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (дата обращения: 2.09.2017).
21. Maritime Security Strategy // European Commission: website. URL: https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en (дата обращения: 12.08.2017).
22. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // EU law and publications: website. URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG (дата обращения: 5.09.2017).
23. Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации”: Утверждено Президентом Российской Федерации 5 декабря 2016 г. // ГАРАНТ: информационно-правовой портал. URL: http://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения: 4.09.2017).

УДК 681.3.067

ОСОБЕННОСТИ РАЗРАБОТКИ СИСТЕМ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ БОРЬБЫ ЗА ЖИВУЧЕСТЬ ПОДВОДНОЙ ЛОДКИ С УЧЕТОМ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Левоева Инга Валерьевна, Мудрова Алёна Александровна
АО «Концерн «НПО «Аврора»
Россия, Санкт-Петербург, ул. Карбышева, 15
e-mails: LevoevaIV@avrora.spb.ru, MudrovaAA@avrora.spb.ru

Аннотация. В докладе рассмотрен подход к разработке систем информационной поддержки борьбы за живучесть на судах ВМФ. Показаны особенности обеспечения информационной безопасности.

Ключевые слова: *система информационной поддержки борьбы за живучесть; информационная безопасность; информационная поддержка.*

THE FEATURES OF THE DEVELOPMENT OF INFORMATION SUPPORT SYSTEMS OF FIGHT FOR SURVIVABILITY OF SUBMARINE WITH THE INFORMATION SECURITY REQUIREMENTS

Levoeva Inga, Mudrova Alena
Concern Aurora Scientific and Production Association JSC,
Russia, St. Petersburg, Carbyshevstr.,15
e-mails: LevoevaIV@avrora.spb.ru, MudrovaAA@avrora.spb.ru

Abstract. The report examines the approach to the development of information support systems of fight for survivability. The features of information security are represented.

Keywords: *information support system of fight for survivability; information security; information support*.

Системы информационной поддержки (СИП) относятся к классу информационных систем и предназначены для формализации и актуализации задач прогнозирования, оценки и управления состоянием корабля и техническими средствами (ТС) при повседневной эксплуатации и при борьбе за живучесть (БЗЖ).

Кроме того, в задачи таких автоматизированных систем (АС) традиционно входит обработка сведений, составляющих государственную тайну, и, следовательно, АС должны соответствовать ряду требований, предъявляемым к автоматизированным системам в защищенном исполнении (АСЗИ).

Разрабатываемые СИП включены в единую информационную сеть комплексной системы управления техническими средствами (КСУ ТС) и располагают всей динамической информацией о технических средствах, действиях операторов и информацией от внешних комплексов, которые классифицируются как центральные координирующие системы управления (ЦКСУ).

С аппаратной точки зрения ЦКСУ – это пультовые стойки, включенные в информационную сеть КСУ ТС. ИП ЦКСУ может располагаться на отсечных приборах и на ноутбуках, включенных в информационную сеть.

К функциям современных ЦКСУ относятся: организация сетевого обмена КСУ ТС прием из СУ ТС и из внешних комплексов массивов информации о состоянии технических средств (включая массивы информации для регистрации); координированное управление ТС через операторов и руководство действиями личного состава отсеков в нормальных режимах эксплуатации и при возникновении аварийной ситуации; формирование, накопление и регистрация информации для анализа работы ТС, действий операторов и ведения вахтенной отчетности; просмотр на мониторе зарегистрированной информации; автоматическое формирование сигналов тревог-команд по каналам колоколо-ревунной сигнализации (КРС) и передача информации о состоянии ТС и решениях по БЗЖ на АРМ КК.

С точки зрения информационной безопасности к функциям ЦКСУ относятся:

– обеспечение безопасного межсетевого взаимодействия с применением сертифицированного программного комплекса межсетевого экранирования (ПК МЭ);

– аутентификация и идентификация непривилегированных (операторы системы) и привилегированных (администратор безопасности и супер-пользователь (root)) пользователей АСЗИ с целью обеспечения защиты от несанкционированного доступа к информации;

– регистрация и учёт событий в системе;

– обеспечение целостности программных средств и обрабатываемой информации;

– сигнализация попыток нарушения защиты:

– периодическое тестирование системы защиты информации от несанкционированного доступа (СЗИ НСД);

– восстановление СЗИ НСД.

Содержательная часть информационной поддержки разрабатывается на основе эксплуатационной документации заказа ЦКБ-проектанта, документации по БЖ и документов МО РФ.

Организационные и технические решения по созданию системы защиты информации в системе информационной поддержки разрабатываются:

– на основании ГОСТ в части защиты информации от НСД в АСЗИ;

– на основании руководящих документов Гостехкомиссии, регламентирующих требования к системе защиты информации и средствам защиты информации;

– на основе требований ТЗ на изделие в части защиты информации;

– на основании приказов МО РФ по обеспечению безопасности информации на объектах МО РФ.

Информационная поддержка обеспечивает выполнение следующих задач:

– представление обобщенных схем систем заказа с отображением текущего состояния основного оборудования и арматуры этих систем и рекомендациями по их переключению в штатные режимы системы;

– формирование рекомендаций КБЧ-5 по управлению ТС при различных аварийных ситуациях;

– представление параметров, необходимых для контроля различных ТС;

– представление информации о расположении помещений по настилам заказа с расположенным на них основным оборудованием;

– автоматизированные модули для расчетных задач.

Комплекс средств защиты системы, в свою очередь, обеспечивает:

– идентификацию, проверку подлинности и контроль доступа субъектов в систему; к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ; к программам; к томам, каталогам, файлам, записям, полям записей;

– управление потоками информации;

– регистрацию и учет входа/выхода субъектов доступа в/из систему (узел сети); запуска/завершения программ и процессов (заданий, задач); доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи; доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей; изменения полномочий субъектов доступа; создаваемых защищаемых объектов доступа;

– учет носителей информации.

– очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей;

– сигнализацию попыток нарушения защиты;

– обеспечение целостности программных средств и обрабатываемой информации.

– физической охраны средств вычислительной техники (сигнализация; установка пломб и др.)

– наличие администратора (службы) защиты информации в АСЗИ;

– периодическое тестирование СЗИ НСД;

– наличие средств восстановления СЗИ НСД;

– экстренное уничтожение машинных носителей информации, содержащей сведения, составляющие государственную тайну;

– использование сертифицированных средств защиты.

Использование СИП повышает эффективность и скорость принятия руководителем БЗЖ правильных решений за счет визуализации расположения помещений и происходящих в них процессов. Расчетные задачи позволяют в кратчайшее время определить критическое состояние и теряемые функции заказа.

При повседневном использовании система предоставляет всю необходимую для контроля и принятия решений динамическую, справочную и расчетную информацию. Соблюдение требований информационной безопасности при разработке АСЗИ, в свою очередь, сохраняет эксплуатационные характеристики системы при внедрении средств защиты.

Решения по защите должны обеспечивать минимально допустимые потери производительности, надежности и удобства управления СИП БЖ.

СПИСОК ЛИТЕРАТУРЫ

1. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России, Москва, 1992.
2. Корчанов В.М., Сус Г.Н., Ушакова Н.П. Опыт НПО «Аврора» по созданию систем информационной поддержки / Системы управления и обработки информации: Научн.-техн. сб./ ОАО «Концерн «НПО «Аврора». СПб, 2010, № 19, с. 93 - 101.

УДК 629.12

УЯЗВИМОСТИ И ЗАЩИТА ANDROIDИIOSПРИЛОЖЕНИЙ

Повечеров Дмитрий Владимирович
Санкт-Петербургский государственный морской технический университет
Россия, Санкт-Петербург, ул. Лоцманская, 3
e-mail: ayluy13mama@list.ru

Аннотация. В работе рассмотрены наиболее распространенные виды атак на Android и Ios приложения и способы решения данной проблемы.

Ключевые слова: *защита, уязвимость, взлом, безопасность.*

WEB APPLICATION SECURITY AND VULNERABILITIES

Povecherov Dmitriy
StateMarineTtechnicalUniversity of St. Petersburg
Russia, St. Petersburg, Lotsmanskaya str., 3
e-mail: ayluy13mama@list.ru

Abstract The paper covers the most common types of attacks on Android and Ios applications and how to solve this problem.

Keywords: *security, vulnerability, break-in, safety.*

Количество вредоносных программ, «заточенных» под атаки на мобильные устройства, в последние годы растет в геометрической прогрессии. И, даже, если вы уверены, что сделали все, чтобы оградить свои гаджеты от проникновения вирусов, вы не можете быть уверены, что их не внедрили еще на заводе или в том же магазине.

Так, исследователи уязвимостей обнаружили предустановленные трояны на устройствах Samsung, LG, Xiaomi, Asus, Oppo и Lenovo. Как же в 21 веке обезопасить свое устройство?

Не секрет, что когда мы пользуемся цифровыми медиа технологиями, то делаем это со смартфона или планшета в 60% времени. К сожалению, это не секрет и для хакеров, которые с каждым днем становятся все изобретательнее.

Одним из наиболее распространенных хакерских методов мобильных атак являются с виду безобидные приложения со скрытыми вирусами. Они могут маскироваться под фоторедакторы, игры и любые другие программы, которые пользуются популярностью. Так же не стоит доверять приложениям из AppStore и Google Play. Поддельные приложения с вредоносным контентом или функциями очень распространены в магазинах приложений, в том числе в официальных. Из-за открытости платформы Android, к сожалению, именно среди Android-приложений чаще встречаются вредоносные экземпляры.

Например, в 2016-2017 году в магазинах Google Play были обнаружены сотни приложений DressCode, которые подключают смартфон к ботнету. Их нашли в 40 приложениях Google Play и 400 из сторонних магазинов. Или VikingHorde и Call Jam — последний был найден в игре «Gems Chest for Clash Royale», количество загрузок которой достигало 400 – 500 тысяч.

Совсем недавно специалисты обнаружили приложения Boost Views и PaxVendor, которые использовались для кражи данных аккаунтов PayPal и Paxful при помощи методов социальной инженерии. Приложения скачали до 100 000 раз. Самый свежий пример — зловред FalseGuide, зашитый в приложения с руководствами по прохождению игр. Некоторые приложения с этим вредоносным кодом появились в Google Play еще в ноябре 2016 года и до апреля этого года успешно избегали обнаружения специалистами по безопасности. По оценкам исследователей, заражено уже около двух миллионов пользователей.

Вредоносные приложения могут получить доступ к файлам на смартфоне, а также собирать данные с помощью фотокамеры, микрофона, фиксации набора с клавиатуры — под угрозой может оказаться личная информация пользователя, включая логины и пароли от мобильного банка и любых других приложений.

Кроме того, они могут генерировать рекламный трафик без ведома пользователя, отправлять СМС на короткие номера, подключать телефон к ботнету.

На первый взгляд подключение смартфона к бот-сети не выглядит трагедией, однако, не стоит недооценивать ботов в своем гаджете. Во-первых, боты очень хорошо маскируются и могут месяцами не выдавать своего присутствия. Во-вторых, с их помощью злоумышленники могут получить полный контроль над устройством и использовать его для масштабных DDoS-атак. Уже известны такие случаи с использованием бытовых устройств интернета вещей — например, атака на провайдера Dyn, в результате которой пропал доступ к таким интернет-гигантам, как Twitter, PayPal, Airbnb, Pinterest, Spotify, GitHub и другим.

Сегодня особенное распространение получили вымогательские зловреды, которые способны заблокировать все данные на устройстве пользователя и требовать выкуп за их восстановление.

Еще один очень важный момент — если вы пользуетесь рабочей почтой с личного мобильного устройства, хакеры вполне могут использовать ваш гаджет как окно в сеть компании, в которой вы работаете. Последствия от такого проникновения могут быть самыми разными, вплоть до серьезных финансовых, репутационных потерь и остановки бизнес-процессов.

Все это и еще много различных типов атак могут вас коснуться. Так как же себя защитить?

В качестве главных мер предосторожности Check Point рекомендует скачивать приложения только из официальных источников и от известных проверенных разработчиков. К сожалению, даже в Google Play попадается множество приложений со вшитыми зловредами, поэтому если у вас есть хоть малейшее сомнение в легитимности, лучше откажитесь от скачивания. Можно ознакомиться с комментариями, поискать информацию о разработчике и приложении в интернете, проверить другие его продукты. Впрочем, даже после тщательной проверки не стоит давать приложению доступ к важным функциям телефона и права администратора. Пользователь должен насторожиться, если, например, обычный калькулятор просит доступ к камере или микрофону. Уже упомянутый зловред FalseGuide при установке запрашивал права администратора устройства, после чего пользователи уже не могли просто удалить его.Наконец, необходимо использовать продукты для мобильной защиты: для хранения ценной информации существуют решения, создающие внутри телефона защищенный контейнер, отделенный от остальной системы. Также существуют различные антивирусные программы и решения для предотвращения мобильных угроз.

Если у вас есть подозрения, что ваш телефон заражен, можно использовать сканеры, определяющие наличие вредоносных программ. На уровне компаний для защиты мобильных пользователей используются решения MDM (Mobile Device Management) или специализированные решения для защиты от вредоносного ПО, такие как Check Point Mobile Threat Prevention.

СПИСОК ЛИТЕРАТУРЫ

1. Журнал "Information Security/ Информационная безопасность" #4, 2013/
2. Попов, А.В. Блог. Новая сфера влияния/ А.В. Попов. –Москва: Манн, Иванов и Фербер, 2008. С.7,8.

УДК 629.12.001.2

ПРАКТИКА ТЕСТИРОВАНИЯ И ВОЗМОЖНОСТИ РАЗВИТИЯ ТЕХНОЛОГИЙ ПК «FORTINET»

Подгорнова Валерия Денисовна
Санкт-Петербургский государственный морской технический университет
Россия, Санкт-Петербург, ул. Лоцманская, 3
e-mail: summer_angel96@mail.ru

Аннотация. В докладе рассмотрены системы обеспечения безопасности ПКFortinet.

Ключевые слова: *развитие; система; безопасность; ПК; брандмауэр.*

PRACTICE OF TESTING AND POSSIBILITY OF DEVELOPMENT OF TECHNOLOGIES OF PC «FORTINET»

Podgornova Valeriya
State MarineTechnical University of St. Petersburg
Russia, St. Petersburg, Lotsmanskaya str., 3
e-mail: summer_angel96@mail.ru

Abstract. This paper discusses security systems for the PCFortinet.

Keywords: *development; system; security; PC; firewall.*

В 2013–2014 гг. многие лидирующие бренды и крупные компании попали на первые страницы газет не благодаря выдающемуся восстановлению после экономического спада или выпуску инновационного продукта, а из-за крупных утечек данных. В ходе лишь одной такой мощной хорошо спланированной атаки были похищены личные данные и/или сведения о кредитных картах более чем 100 миллионов клиентов.

Эти атаки привлекают к себе наибольшее внимание потребителей, законодателей и СМИ, когда их объектами становятся крупные организации с профессиональными службами безопасности и разветвленной инфраструктурой защиты от злоумышленников. Однако никто не может чувствовать себя в полной безопасности: небольшие структуры также становятся жертвами масштабных скоординированных атак или вредоносных программ.

Быстрое развитие виртуальной экономики и взрывное увеличение объема трафика в корпоративных инфраструктурах побуждают ведущие предприятия к внедрению высокоэффективной технологии ASIC (специализированные интегральные микросхемы), которая позволяет адаптироваться к растущим требованиям и сохранить конкурентное преимущество. С момента создания компания Fortinet развивала ASIC и продолжает создавать инновационные решения для

защиты, в число которых входит процессор следующего поколения FortiASIC SOC3, предназначенный для обеспечения безопасности.

Решение FortiASIC SOC3 обеспечивает работу новых межсетевых экранов для распределенных компаний серии Fortinet FortiGate 60E, которые устанавливают новый уровень, являясь самыми мощными межсетевыми экранами в своем классе. Характеристики межсетевых экрановFortinet превышают показатели доступных на рынке решений конкурентов. Средство FortiGate 60E идеально подходит для распределенных компаний, филиалов, а также предприятий малого и среднего бизнеса, так как благодаря адаптивной системе сетевой безопасности Fortinet обеспечивает эффективную защиту, высокую производительность сети и простую реализацию функций отслеживания и управления в рамках единой системы. В рамках решений серии FortiGate 60E множество функций обеспечения безопасности и работы сети объединено в рамках одного компактного инструмента

Средство Fortinet SOC3 разработано на основе современных достижений в сфере проектирования кристаллов, которые позволили объединить процессоры, обеспечивающие работу сетей и систем безопасности, с четырехъядерным ЦП в рамках одного кристалла. Адаптированная к нуждам безопасности архитектура средства SOC3 обеспечивает реализацию функций глубокого анализа и проверки на уровне, который соответствует характеристикам корпоративных и универсальных ЦП, обеспечивающих работу продуктов компаний-конкурентов, и даже превышает их. Также эта архитектура обладает эффективной структурой, которая сокращает энергопотребление до 5 Вт и позволяет обойтись без вентилятора, что способствует снижению уровня шума. Благодаря этому наше решение подходит для развертывания в любой среде.

СПИСОК ЛИТЕРАТУРЫ

1. Сервис ИТ. Fortinet[Электронный ресурс], URL: https://kservis-it.ru/info/brands/fortinet/ (Дата обращения: 24 сентября 2017).
2. Официальный сайт "Fortinet" [Электронный ресурс] URL: https://www.fortinet.com/solutions.html (Дата обращения: 24 сентября 2017).
3. Блог "Fortinet" [Электронный ресурс], URL:https://blog.fortinet.com/?_ga=2.47786788.200774133.1506717699-1792742136.1506717699 (Дата обращения: 24 сентября 2017).

УДК 621.192, 623.9, 681.518

ВИЗУАЛИЗИРОВАННЫЕ ЛОГИКО-ВЕРОЯТНОСТНЫЕ МОДЕЛИ СТРУКТУРНО-СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ

Поленин Владимир Иванович, Сущенков Дмитрий Андреевич
Военный учебно-научный центр ВМФ «Военно-морская академия»
Россия, Санкт-Петербург, Ушаковская наб., 17/1
e-mails: polenin@mail.ru, sushenkov_dmitri@mail.ru

Аннотация. В работе решается актуальная задача системного анализа, связанная с созданием модульных визуализированных логико-вероятностных моделей элементов, с использованием которых облегчается сборка структурных схем функционирования структурно-сложных объектов и систем в целом. Модульные структурные схемы отвечают требованиям унификации и комбинированного отражения влияния одновременно всех основных обычно учитываемых факторов и свойств. Визуальное программирование позволяет программировать, используя графические или символьные элементы, которыми можно манипулировать согласно некоторым правилам. Полученные результаты позволяют пользователям общего логико-вероятностного метода (ОЛВМ) создавать модели с требуемыми целевым назначением и свойствами, что обычно представляет собой значительные трудности

Ключевые слова: *структурно-сложные объекты и системы; неблагоприятные и поражающие факторы; логико-вероятностные модели и методы; показатели надежности; эффективности и риска*.

VISUALIZED LOGICAL-PROBABILISTIC MODELS OF STRUCTURALLY COMPLEX TECHNICAL SYSTEMS

PoleninVladimir, Sushchenkov Dmitry
Russia, St. Petersburg, Ushakov nab., 17/1
Military educational scientific center of Navy "Naval Academy"
e-mails: polenin@mail.ru, sushenkov_dmitri@mail.ru

Abstract. Inpaper the relevant problem of the system analysis connected with creation of the modular visualized logiko-probabilistic models of elements with which use assembly of block diagrams of functioning of structural and difficult objects and systems in general is facilitated is solved. Modular block diagrams meet the requirements of unification and the combined influence reflection of at the same time all major usually considered factors and properties. Visual programming allows to program, using graphic or symbolical elements which can be manipulated according to some rules. The received results allow users of the general

logiko-probabilistic method (GLPM) to create models with the required purposes and properties that usually represents considerable difficulties

Keywords: *structurally complex objects and systems; and adverse effects; of logical-probabilistic models and methods; reliability; efficiency and risk.*

Одной из важных задач системного анализа структурно-сложных объектов является задача создания модульных структурных схем функционирования элементов, с использованием которых облегчается сборка структурных схем функционирования структурно-сложных объектов и систем в целом. В частности, именно на такой подход к созданию структурных схем функционирования структурно-сложных объектов и систем ориентирован программный комплекс автоматизированного структурного моделирования ПК АСМ «АРБИТР» [1], реализующий информационную технологию ОЛВМ [4].

При этом задача системного анализа функционирования структурно-сложных объектов состоит в создании таких структурных схем функционирования элементов и систем, которые комбинированно отражали бы влияние одновременно всех основных обычно учитываемых факторов и свойств и позволяли бы вычислять системные характеристики систем одновременно по всем основным обычно интересующим показателям.

К числу обычно учитываемых факторов и свойств технических систем относятся техническая безотказность элементов системы, воздействие внешних неблагоприятных факторов, стойкость элементов к этому воздействию и характер аварийных отказов (с развитием или без развития аварии). К числу обычно интересующих показателей относятся показатели устойчивости их функционирования и риска (ожидаемого ущерба), связанного с воздействием неблагоприятных внешних факторов.

Следует отметить, что при применении известных сетевых методов и программных комплексов, использующих логико-вероятностные методы, например, RELAX, Risk Spectrum и др., решение задачи создания единых моделей, учитывающих как нормальные условия функционирования, так и внешние неблагоприятные и поражающие факторы, является недоступным.

Второй задачей методического обеспечения моделирования, решение которой обеспечивается программным комплексом «АРБИТР», является задача визуального программирования – способа создания программ путем манипулирования графическими объектами вместо написания кода в текстовом виде. Визуализированное моделирование представляет собой подобие термина «Визуальное программирование», принятого в информационных технологиях [3, 5].

Примером может являться унифицированный язык моделирования UML (англ. Unified Modeling Language) в области разработки программного обеспечения моделирования бизнес-процессов. Другими примерами языков визуального программирования являются: Microsoft Visual Programming Language, язык для робототехники, Simulink MATLAB, AnyLogic.

MS Visual Studio и Delphi является визуальными средами программирования, но не визуальными языками программирования.

Следует обратить внимание на то, что как ОЛВМ, так и упомянутые выше программные средства имеют предметной областью модели, которые можно отразить ориентированными графами. В ОЛВМ, AnyLogic и исследовании операций такого рода модели являются событийными моделями третьего уровня.

ОЛВМ при поддержке ПК АСМ также представляет собой систему визуального программирования, которая базируется на графическом отображении модели в форме ориентированных графов. Эту систему можно расширить до уровня визуализированного моделирования, что представляет собой ориентированные графы, элементы которых совмещаются с элементами графической формы модели вооруженной борьбы. В этом и состоит сущность предлагаемой информационной технологии.

Разработан комплекс визуализированных логико-вероятностных моделей, обеспечивающий пользователю ОЛВМ сборку необходимых моделей по некоторым формальным правилам.

В качестве примера рассмотрена модель и методика функционирование топливного трубопровода в агрессивной (опасной) среде, которые легко воспроизводятся визуальными средствами ОЛВМ. После их создания средствами ОЛВМ задача анализа устойчивости функционирования и риска (ожидаемого ущерба) исследуемой системы, связанных с воздействием неблагоприятных внешних факторов, решается автоматически. Адекватность итоговой схемы понятиям и состояниям полной устойчивости и полного риска и корректность ее логической реализации подтверждаются тем, что эти состояния-антиподы образуют полную группу событий и сумма их вероятностей удовлетворяет условию нормировки (равенства единице).

Таким образом:

1. Решена одна из важных задач системного анализа структурно-сложных объектов – задача создания модульных структурных схем функционирования элементов, с использованием которых облегчается сборка структурных схем функционирования структурно-сложных объектов и систем в

целом. Результаты решения задачи ориентированы на информационную технологию ОЛВМ, реализованную в программных комплексах ПК АСМ 2001 и «АРБИТР».

2. Разработан комплекс визуализированных логико-вероятностных моделей процесса вооруженной борьбы, обеспечивающий пользователю ОЛВМ сборку необходимых моделей по некоторым формальным правилам.Полученные результаты обеспечивают реализацию принципа доступности методов и технологии ОЛВМ для широкого круга пользователей и способствуют объективизации системных исследований структурно-сложных опасных производственных объектов и вооруженного противоборства.

СПИСОКЛИТЕРАТУРЫ

1. АРБИТР, Программный комплекс автоматизированного структурно-логического моделирования и расчета надежности и безопасности систем (ПК АСМ СЗМА) базовая версия 1.0 / Автор Можаев А.С. Правообладатель ОАО «СПИК СЗМА». // Свидетельство об официальной регистрации № 2003611101. − М.: РОСПАТЕНТ РФ, 2003.
2. Волгин Н.С., Махров Н.В., Юровский В.А. Исследование операций. Часть I. - Л.: ВМОЛА, 1978. - 301 с.
3. Моисеев Н.Н. Математические задачи системного анализа. – М.: Наука, 1981, 488с.
4. Поленин В.И., Рябинин, И.А., Свирин С.К., Гладкова И.А. Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства // Монография, научное издание / Под ред. А.С. Можаева. – СПб: СПб-региональное отделение РАЕН, 2011. − 416 с.
5. Визуальное программирование: URL: http://life-prog.ru/view_zam2.php?id=162/ – 2017.

УДК 621.192, 623.9, 681.518

МЕТОДИКА ПОСТРОЕНИЯ ЛОГИКО-ВЕРОЯТНОСТНЫХ МОДЕЛЕЙ СТРУКТУРНО-СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ ДЛЯ ОЦЕНКИ РИСКА И БЕЗОПАСНОСТИ ИХ ФУНКЦИОНИРОВАНИЯ

Поленин Владимир Иванович, Потехин Александр Алексеевич
Военный учебно-научный центр ВМФ «Военно-морская академия»
Россия, Санкт-Петербург, Ушаковская наб., 17/1
e-mails: polenin@mail.ru, nconr212@yandex.ru

Аннотация. В статье решается актуальная задача системного анализа, связанная с созданием модульных логико-вероятностных событийных структурных моделей функционирования элементов, с использованием которых облегчается сборка структурных моделей функционирования структурно-сложных объектов и систем в целом. Модульные структурные модели отвечают требованиям унификации по отношению к техническим системам и комбинированного отражения влияния одновременно всех основных обычно учитываемых факторов и свойств.

Ключевые слова: *структурно-сложные объекты и системы; неблагоприятные и поражающие факторы; логико-вероятностные модели и методы; показатели надежности; эффективности и риска*.

METHODOLOGY FOR CONSTRUCTION OF LOGIC-PROBABILISTIC MODELS OF STRUCTURALLY COMPLEX TECHNICAL SYSTEMS FOR RISK ASSESSMENT AND SAFETY OF THEIR FUNCTIONING

Polenin Vladimir, Potekhin Alexander
Military educational and scientific center of the Navy "Naval Academy"
Russia, St. Petersburg, Ushakovskaya nab., 17/1
e-mails: polenin@mail.ru, nconr212@yandex.ru

Abstract. The article deals with the actual problem of system analysis associated with the creation of modular logic-probabilistic event structural models of the functioning of elements, with the use of which it is easier to assemble structural models for the functioning of structurally complex objects and systems as a whole. Modular structural models meet the requirements of unification in relation to technical systems and combined reflection of the influence of all the main commonly taken factors and properties.

Keywords: *structurally complex objects and systems; adverse and damaging factors; Logical-probabilistic models and methods; reliability indicators; efficiency and risk.*

Устойчивость как структурное качество систем

Ниже рассматривается структурное представление свойства устойчивости применительно к техническим системам, поскольку его элементы имеют определения, установленные ГОСТ.

Устойчивость – способность системы в процессе изменений, вызываемых различными причинами, сохранять свойства работоспособности и/или безопасности.

Устойчивость технических систем является комплексным качеством, включающим в себя следующие составляющие –структурные свойства [5]:

– надежность (безотказность);
– стойкость (условная живучесть);
– живучесть (полная);

– технический риск.

Структурная надежность (безотказность) технической системы − способность системы сохранять работоспособность при случайных возникновениях отказов/восстановлений ее элементов в нормальных (заданных) условиях эксплуатации.

Структурная стойкость − свойство системы сохранять работоспособность в условиях достоверного возникновения поражающих факторов.

Структурная живучесть − способность системы сохранять работоспособность в условиях случайного возникновения поражающих факторов.

Структурная устойчивость − способность системы сохранять работоспособность, определяемая различными совместными комбинациями свойств структурной надежности и живучести.

Условная (идеальная) эффективность − способность системы реализовать свое функциональное предназначение (цель функционирования и т.п.) при достоверном нахождении в состоянии работоспособности.

Реальная эффективность − способность системы реализовать свое функциональное предназначение (цель функционирования и т.п.) при ее устойчивости.

Риск аварии − мера опасности, характеризующая:

– возможность случайного возникновения аварий и отказов системы с различными уровнями последствий;

– тяжесть (уровень, ожидаемый ущерб) последствий различных аварий и отказов системы.

Технический риск − вероятность возникновения аварии вследствие отказов элементов системы, с последствиями определенного уровня (класса) за определенный период функционирования.

Ущерб от аварии − потери (убытки), вред окружающей среде и производственной сфере вследствие достоверного возникновения аварии (поражающего воздействия) данного вида.

Ожидаемый ущерб − математическое ожидание величины ущерба от возможных аварий (поражающих воздействий) за определенное время.

Расчет показателей структурных свойств осуществляется на математических моделях структурно-сложных систем, особенностями которых являются отражение взаимосвязей элементов и событийный характер.

Рис. 1. Структурное представление свойства устойчивости

Постановка задачи

Одной из важных задач системного анализа структурно-сложных объектов является задача создания модульных структурных моделей функционирования элементов, с использованием которых облегчается сборка структурных моделей функционирования структурно-сложных объектов и систем в целом. В частности, именно на такой подход к созданию структурных моделей функционирования структурно-сложных объектов и систем ориентирован программный комплекс «АРБИТР» [2], реализующий информационную технологию ОЛВМ [4].

Другая важная задача системного анализа функционирования структурно-сложных объектов состоит в создании таких структурных моделей функционирования элементов и систем, которые комбинированно отражали бы влияние одновременно всех основных обычно учитываемых факторов и свойств и позволяли бы вычислять системные характеристики систем одновременно по всем основным обычно интересующим показателям.

К числу обычно учитываемых факторов и свойств относятся техническая безотказность элементов системы, воздействие внешних неблагоприятных факторов, стойкость элементов к этому воздействию и характер аварийных отказов (с развитием или без развития аварии).

К числу обычно интересующих показателей технических систем и опасных производственных объектов (ОПО) относятся показатели устойчивости их функционирования и риска (ожидаемого ущерба), связанного с воздействием неблагоприятных внешних факторов.

Следует отметить, что при применении известных сетевых методов и программных комплексов, использующих логико-вероятностные методы, например, RELAX, Risk Spectrum и др., решение задачи создания единых моделей, учитывающих как нормальные условия функционирования, так и внешние неблагоприятные и поражающие факторы, является недоступным. Дело в том, что в этих методах и программных комплексах реализован неполный базис логических операций, с помощью которых представляются логические функции. В соответствующих классических в блок-схемах и в деревьях отказов логико-вероятностных моделей такой базис включает только две логические операции «И» и «ИЛИ». Эта часть функций алгебры логики охватывает класс так называемых монотонных логических моделей устойчивости систем.

Именно так обстоит дело с решением задачи прогнозирования риска опасных производственных объектов (ОПО) в условиях гипотетических повреждений в примере аварии хранилища горюче-смазочных материалов [5]. Здесь модель аварии, вызванной разрушением (или поражением) хранилища горюче-смазочных материалов, представляется с помощью дерева событий, причем совершенно отдельно от модели функционирования самого объекта в нормальных условиях эксплуатации.

Однако в области системных исследований, связанных с управлением реальным функционированием объектов, актуальной является задача комплексного учета влияния неблагоприятных и поражающих факторов непосредственно на моделях текущего функционирования объектов.

Для решения такой задачи наиболее подходящим методом является Общий логико-вероятностный метод, использующий функционально полный набор логических операций «И», «ИЛИ» и «НЕ» (инверсия), позволяющий реализовать все функциональные возможности основного аппарата моделирования – алгебры логики.

Первым этапом решения этой задачи является создание событийных унифицированных модульных моделей функционирования отдельных элементов, отражающих влияние неблагоприятных и поражающих факторов. Полагая основные положения ОЛВМ известными, модели функционирования целесообразно представлять сразу в виде схем функциональной целостности (СФЦ), тем более, потому, что графически они полностью совпадают со схемами функционирования в форме ориентированных графов. Технология объединения СФЦ отдельных элементов в СФЦ структурно-сложных систем является известной [4].

Модульная модель функционирования элемента технической системы с комбинированным учетом влияющих факторов

Для наглядности модельных разработок рассмотрим схему функционирования элемента, под которым для примера будем понимать функционирование топливного трубопровода в агрессивной (опасной) среде (рис. 2). Все вершины СФЦ представляют собой определенные события.

Наличие опасности аварийного развития событий – стандартная характеристика опасных производственных объектов (ОПО).

Учет первого фактора.

В функциональной вершине 2 задается вероятность воздействия внешнего неблагоприятного фактора. Пусть вершина 2 – событие воздействия по трубопроводу, по каким-либо причинам, внешнего неблагоприятного фактора, например, ударное. Вероятность его появления, как вероятность неблагоприятного стечения обстоятельств, считаем известной, она определяется расчетным путем по условиям функционирования элемента P(y2)=0.1.

Учет второго фактора.

Функциональная вершина 3 характеризует нестойкость трубопровода к воздействию внешнего неблагоприятного фактора. Тогда прямой выход y3 будет соответствовать проявлению трубопроводом свойства нестойкости или аварийного отказа, а инверсный выход y"3 – проявлению трубопроводом свойства стойкости.

Пусть стойкость трубопровода характеризуется определенной и известной вероятностью Pc=0.4. Вероятность нестойкости 1–Pc=0.6 задается в функциональной вершине 3.

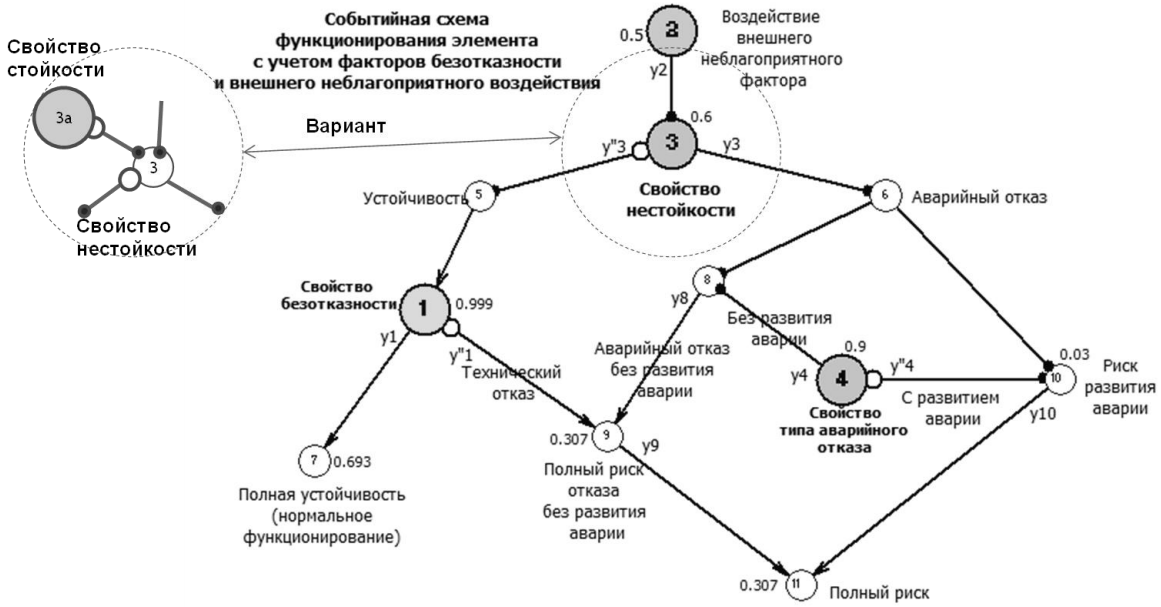


Рис. 2. СФЦ функционирования элемента технической системы с комбинированным учетом влияющих факторов

Проявление свойства стойкости y"3 с вероятностью

$$P(y"3)=1-[P(y2)(1-Pc)]=1-0.1\cdot 0.6=0.94$$

формально соответствует функционированию элемента в нормальных условиях. Наступает событие 5 устойчивости элемента к воздействию внешнего неблагоприятного фактора.

Учет третьего фактора.

В функциональной вершине 1 задается вероятность безотказной работы элемента.

Формально, при сохранении нормальных условий функционирования элемента (вершина 5) и проявлении им свойства безотказности (вершина 1) наступает событие нормального функционирования или состояние полной устойчивости элемента (прямой выход y1 к вершине 7). В противоположном случае наступает событие технического отказа (инверсный выход y"1 к вершине 9).

Учет четвертого фактора.

В функциональной вершине 4 задается вероятность аварийного отказа элемента без развития аварии. Если проявляется свойство нестойкости трубопровода к воздействию внешнего неблагоприятного фактора и наступает аварийный отказ (событие y3 с переходом к вершине 6), то могут иметь место два исхода, представленных вершиной-событием 4:

– прямой выход – событие y4 повреждения и отказа трубопровода без развития аварии, например, при таком типичном следствии удара по трубопроводу, как его смятие и, вследствие этого, утрата транспортной пропускной способности;

– инверсный выход – событие y"4 повреждения и отказа трубопровода с развитием аварии, например, вследствие разрушения оболочки трубопровода.

Произведение в вершине 8 событий y3 нестойкости трубопровода к удару и y4 смятия оболочки трубопровода с утратой транспортной пропускной способности представляет собой наступление события y8 аварийного отказа трубопровода без развития аварии.

Произведение в вершине 10 событий y3 нестойкости трубопровода к удару и y"4 разрушения оболочки трубопровода с развитием аварии представляет собой наступление события y10 аварийного отказа трубопровода с развитием аварии. Соответственно, вероятность наступления события y10 представляет собой вероятность риска развития аварии, а в произведении на сумму материального ущерба (с учетом тяжести последствий) – полный риск аварии согласно ГОСТ.

Смятие и разрушение оболочки трубопровода как следствия его нестойкости к удару, могут быть изучены и оценены в вероятностной мере, например, по потенциальной частости их наступления в эксперименте или по соотношению показателей устойчивости к смятию и разрушению, полученных методами теории сопротивления материалов.

Пусть смятие и разрушение оболочки трубопровода наступают в соотношении 4:1, тогда выходам вершины 4 соответствуют вероятности P(y4)=0.8 и P(y"4)=0.2.

Свойства-события 3 – нестойкость трубопровода к удару, как условие возникновения повреждения трубопровода, и 4 – характер повреждения, являются независимыми между собой. Тогда вероятности наступления событий y8 аварийного отказа трубопровода без развития аварии и y10 аварийного отказа трубопровода с развитием аварии будут представлять собой, с учетом несовместности случайных событий y4 и y"4, значения P(y8)=0.048; P(y10)= 0.012.

Далее, событие y8 отказа без развития аварии и технический отказ y"1 трубопровода по физическому смыслу однородны и потому могут быть объединены в вершине-событии 9, характеризующем полный риск отказа без развития аварии. Вероятность его наступления P(y8)=0.048.

Наконец, сочетание полного риска отказа без развития аварии (y9) и риска развития аварии (y10), с учетом несовместности случайных событий y3 и y"3, получит значение приводят к понятию полного риска (y11) с вероятностью P(y9)=0.0694.Адекватность представленной модели понятиям и состояниям полной устойчивости и полного риска и корректность ее логической реализации подтверждаются тем, что эти состояния-антиподы образуют полную группу событий и сумма их вероятностей удовлетворяет условию нормировки (равенства единице).

Пример формирования СФЦ структурно-сложного объекта с помощью модульной модели функционирования элемента технической системы с комбинированным учетом влияющих факторов

Ниже приводится пример части схемы системы выгрузки ГСМ из танков (рис. 3). Требуется составить СФЦ этой системы с помощью рассмотренной выше модульной модели функционирования элемента технической системы.

Система состоит из танка, трубопровода, насоса, двух клапанов и приемника ГСМ.

Используя модульную СФЦ (см. рис. 2) последовательно для всех элементов системы, получим СФЦ функционирования системы в целом (рис. 4).Нестойкости к внешнему неблагоприятному фактору приняты различными для клапанов и насоса.Этим демонстрируется возможность индивидуального или группового подхода к учету каждого из влияющих факторов по всем элементам структурно-сложной системы.

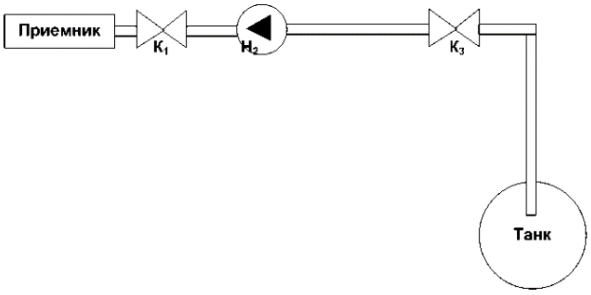


Рис. 3. Схема системы выгрузки ГСМ из танков

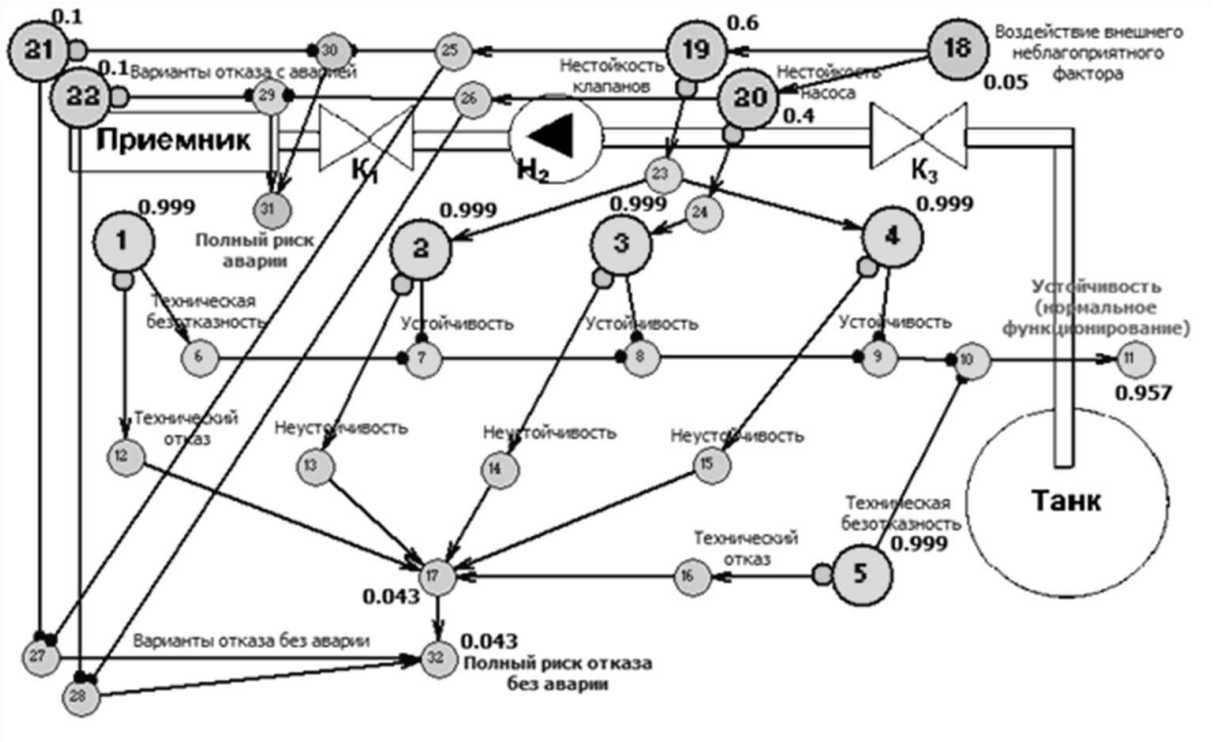


Рис. 4. СФЦ системы выгрузки ГСМ из танков

Достоверность итоговой СФЦ и результатов моделирования подтверждается выполнением условия нормировки, а именно, равенства единице суммы показателей устойчивости (вершина 11) и полного риска (вершина 17).

Выводы.

1. Решена одна из важных задач системного анализа структурно-сложных объектов – задача создания модульных структурных моделей функционирования элементов, с использованием которых облегчается сборка структурных моделей функционирования структурно-сложных объектов и систем в целом. Результаты решения задачи ориентированы на информационную технологию ОЛВМ, реализованную в программных комплексах ПК АСМ 2001 и «АРБИТР» [2].

2. Разработаны структурные модели функционирования элементов, которые комбинированно отражают влияние одновременно всех основных обычно учитываемых факторов и свойств технических систем и позволяют вычислять системные характеристики этих систем одновременно по всем основным обычно интересующим показателям.

3. Полученные результаты обеспечивают реализацию принципа доступности методов и технологии ОЛВМ для широкого круга пользователей и способствуют объективизации системных исследований структурно-сложных опасных производственных объектов.

СПИСОКЛИТЕРАТУРЫ

1. Автоматизация процессов борьбы за живучесть корабля, судна // Коллективная открытая монография. – СПб: Координационный совет НП «ИАП БЖКС». – 2014.
2. АРБИТР, Программный комплекс автоматизированного структурно-логического моделирования и расчета надежности и безопасности систем (ПК АСМ СЗМА) базовая версия 1.0 / Автор Можаев А.С. Правообладатель ОАО «СПИК СЗМА». // Свидетельство об официальной регистрации № 2003611101. − М.: РОСПАТЕНТ РФ, 2003.
3. Волгин Н.С., Махров Н.В., Юровский В.А. Исследование операций. Часть I. - Л.: ВМОЛА, 1978. - 301 с.
4. Поленин В.И., Рябинин, И.А., Свирин С.К., Гладкова И.А. Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства // Монография, научное издание / Под ред. А.С. Можаева. – СПб: СПб-региональное отделение РАЕН, 2011. − 416 с.
5. РД 03-418-01. Методические указания по проведению анализа риска опасных производственных объектов // Нормативные документы межотраслевого применения по вопросам промышленной безопасности и охраны недр. Выпуск 10. М.: ГУП «НТЦ ПБ» Госгортехнадзора России, 2001. - 60с.

УДК 621.192

КОМПЬЮТЕРНЫЕ ВИРУСЫ: ИСТОРИЯ, КЛАССИФИКАЦИЯ, ПРОТИВОДЕЙСТВИЕ

Цыганков Илья Александрович
Санкт-Петербургский государственный морской технический университет
Россия, Санкт-Петербург, ул. Лоцманская, 3
e-mail: pegas19962010@mail.ru

Аннотация. В докладепредставлены материалы по по истории возникновения и классификации компьютерных вирусов по степени опасности (негативноговоздействия)на операционную
систему и компьютер в целом, обсуждаются вопросы выявления наиболее опасных вирусов и противодействия им.

Ключевые слова: *компьютерный вирус; электронная угроза; антивирусные программы.*

COMPUTER VIRUSES: HISTORY, CLASSIFICATION, OPPOSITION

Tsygankov Ilya
State Marine Ttechnical University of St. Petersburg
Russia, St. Petersburg, Lotsmanskaya str., 3
e-mail: pegas19962010@mail.ru

Abstract. The report presents materials on the history and classification of computer viruses according to the degree of danger (negative impact) on the operating system and the computer as a whole, discusses the identification of the most dangerous viruses and counteracting them.

Keywords: *computer virus; electronic threat; anti-virus programs.*

Компьютерные вирусы — самая известная и распространённая электронная угроза. Практически каждый пользователь компьютера рано или поздно сталкивается с ней, но зачастую не имеет комплексного представления, что представляют собой компьютерные вирусы, каким путём они заражают систему, как размножаются, чем отличаются друг от друга и как с ними бороться, принимая во внимание способность вирусов к размножению и выполнению без ведома пользователя иных целенаправленных действий, наносящих вред пользователю и компьютеру.

Впервые самовоспроизводящиеся программы были описаны ещё Джоном фон Нейманом в 1951 году. Одна из первых моделей такой программы была описана супругам Пенроуз в статье для журнала «Nature» в 1957 году. Первым «настоящими» вирусами считаются программы для

компьютеров «Apple», появившиеся в 1977 году и умевшие объединяться в сеть. Впервые серьёзная «эпидемия вирусов» случились в 1987 году. Вирус «Brain» («Пакистанский вирус»), написанный братьями Амджатом и Базитом Алви, был обнаружен летом 1987 года, когда эпидемия поразила 18 тысяч компьютеров в США.

Компьютерные вирусы можно классифицировать по среде обитания, по способам проникновения и заражения, по вредоносным действиям и по особенностям функционирования. В компьютер вирусы могут проникать через внешние накопители, электронную почту, систему обмена мгновенными сообщениями, Интернет, локальные сети и др. Существует большое количество видов вирусов: рекламные программы (проникают в компьютер пользователя через рекламные продукты), бэкдоры (вирусы, которые устанавливает взломщик на взломанном им компьютере после получения первоначального доступа с целью повторного получения доступа к системе), полиморфные вирусы (вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совладать ни в одном бите) и многие другие.

В настоящий момент существует множество антивирусных программ. Компании, разрабатывающие антивирусные программы, кладывют в индустрию значительные средства, онако не дают гарантии, что они смогут справиться с новейшими вирусными разработками.

В докладепредставлена сравнительная классификации компьютерных вирусов по степени опасности (негативного воздействия) на операционную систему и компьютер в целом, а также обсуждаются вопросы выявления наиболее опасных вирусов и противодействия им.

СПИСОК ЛИТЕРАТУРЫ

24. Википедия [Электронный ресурс]/ URL: https://ru.wikipedia.org/wiki/ - (Дата обращения 02.10.2017).
25. Компьютерные вирусы [Электронный ресурс]/ URL: http://comp.web-3.ru/virus/?act=full&id_article=1411 - (Дата обращения 02.10.2017).
26. Компьютерные вирусы и методы борьбы с ними [Электронный ресурс]/ URL: https://studopedia.ru/10_257946_kompyuternie-virusi-i-metodi-borbi-s-nimi.html- (Дата обращения 02.10.2017).

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОЛОГИИ

УДК 551.593

ЗАТМЕННОЕ ЗОНДИРОВАНИЕ ВЕРХНЕЙ АТМОСФЕРЫ ЗЕМЛИ С ПИЛОТИРУЕМОЙ ОРБИТАЛЬНОЙ СТАНЦИИ: ПОЛУЧЕНИЕ И СОХРАНЕНИЕ ИНФОРМАЦИИ

Бузников Анатолий Алексеевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Россия, Санкт-Петербург, ул. Профессора Попова, 5
e-mail: aabuznikov@mail.ru

Аннотация. Приведены результаты эксперимента по затменному зондированию атмосферы с пилотируемой орбитальной станции для исследования вертикального распределения малых газовых компонентов. Рассмотрены возможности получения и сохранения информации о глобальном состоянии верхней атмосферы Земли.

Ключевые слова: *затменное зондирование атмосферы; спектрофотометрия; концентрация водяного пара.*

ECLIPSING REMOTE SENSING OF THE EARTH'S UPPER ATMOSPHERE FROM MANNED SPACECRAFT: OBTAINING AND SAVING THE INFORMATION

Buznikov Anatoliy
St. Petersburg State Electrotechnical University «LETI»
Russia, St. Petersburg, Professor Popovstr.,5
e-mail: aabuznikov @mail.ru

Abstract. Results of the experiment on the eclipsing remote sensing of the Earth's upper atmosphere are given. The paper describes the opportunities for obtaining and saving the information on the global state of the upper atmosphere.

Keywords: *eclipsing remote sensing of the atmosphere; spectrophotometry; water vapor concentration.*

Среднесрочный и долгосрочный прогнозы погоды для отдельных регионов базируются на информации о глобальном состоянии атмосферы. Причём большое значение имеет информация о распределении концентрации малых газовых компонентов, таких как водяной пар, озон, окислы азота и др., в верхних слоях атмосферы. Они непосредственно взаимодействуют с солнечным излучением и влияют на его поглощение и перенос в атмосфере.

Разработка методов и аппаратуры для постоянного слежения за распределением малых газовых компонентов в стратосфере и мезосфере важна для практического претворения в жизнь Всемирной климатической программы [1]. Интерес к изучению распределения малых газовых компонентов вызван также возрастающим уровнем загрязнения атмосферы, важностью изучения фотохимических процессов в стратосфере и мезосфере, поисками зависимостей между пространственно-временными вариациями газовых и аэрозольных компонентов атмосферы и современными изменениями климата [2]. Изменение концентрации малых газовых компонентов может вызвать нарушение естественных процессов, протекающих в атмосфере, и различные нарушения экологического равновесия. Например, увеличение содержания водяного пара приведёт к изменению альбедо системы Земля – атмосфера. Сведения о вертикальном распределении водяного пара необходимы также для построения строгой теории теплового режима стратосферы и мезосферы.

Глобальный характер поставленной задачи потребовал разработки новых методов измерений с использованием средств космической техники, позволяющих осуществлять систематическое дистанционное слежение за состоянием атмосферы в планетарном масштабе. При этом весьма перспективен метод затменного зондирования атмосферы на скользящих оптических трассах при восходах и заходах Солнца относительно космического аппарата, на котором устанавливается спектрометр, регистрирующий поглощение солнечной радиации в отдельных, наиболее информативных полосах поглощения исследуемых атмосферных газов. Схема проведения эксперимента по затменному зондированию приведена на рис. 1.

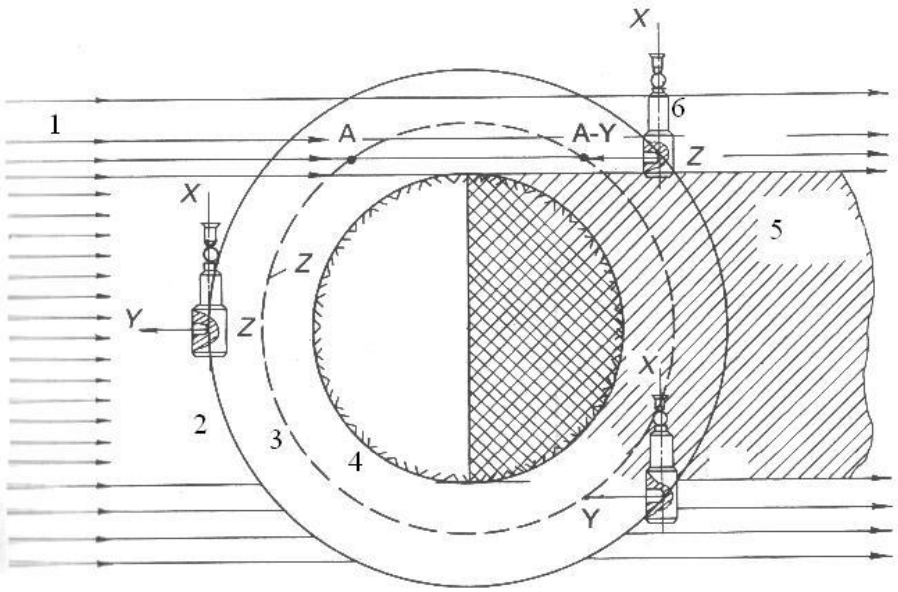


Рис. 1. Схема проведения эксперимента по затменному зондированию: 1 – солнечные лучи; 2 – орбита станции; 3 – условная верхняя граница атмосферы; 4 – поверхность Земли; 5 – тень Земли; 6 – пилотируемая орбитальная станция.

Впервые конкретная реализация метода затменного зондирования атмосферы для изучения вертикального распределения водяного пара была осуществлена во время полета орбитальной станции «Салют-4» [3], на борту которой был установлен комплекс солнечных спектрометров КСС-2. Это был первый в мировой практике негерметизированный спектрометр высокого разрешения, работавший за пределами герметичного корпуса станции в условиях высокого вакуума. С помощью КСС-2 впервые была реализована схема затменного зондирования атмосферы Земли и получены достоверные данные о вертикальном распределении водяного пара в стратосфере и мезосфере на высотах от 30 до 60 км.

Солнечная следящая система наводила входные щели спектрометров на геометрический центр солнечного диска с точностью до одной угловой минуты и удерживала их в таком положении во время проведения измерений. Параллельностьвходных щелей спектрометров к горизонту Земли в момент измерений осуществлялась за счет ориентации станции, совершающей поступательное движение в инерциальном режиме. Блок спектрометров КСС-2 был установлен за пределами герметичного корпуса станции «Салют-4» и включал в себя инфракрасный (ИК) спектрометр со спектральным каналом шириной 3800–3825 $см^{-1}$ и полушириной аппаратной функции 0,8 $см^{-1}$. Он осуществлял измерение поглощения солнечного излучения в 2,7 мкм полосе водяного пара. Ультрафиолетовый (УФ) спектрометр имел спектральный диапазон измерений 400 Å в области от 2000 до 3000 Å со спектральной шириной щели 2 Å. Спектрометр обладал высоким быстродействием. При измерении поглощения водяным паром в полосе 2,7 мкм каждый спектр шириной 3800–3825 $см^{-1}$ вместе с калибром записывается за 1,75 с, а контур основной информативной линии 3816,07 $см^{-1}$ – за 0,09 с.

На рис. 2 приведен пример записи спектров поглощения водяного пара на восходе Солнца. Измерения отношения смеси водяного пара в стратосфере и мезосфере, проведенные в зимний период над Маршалловыми островами, свидетельствуют о наличии сухой стратосферы с отношением смеси q_{H2O} = (2–28)×10^{-6} г/г на высотах от 30 до 60 км. Результаты детальной обработки полученных данных приведены в работе [4]. В дальнейшем разработанная методика затменного зондирования была успешно использована американцами при создании и запуске спутника UARS [5].

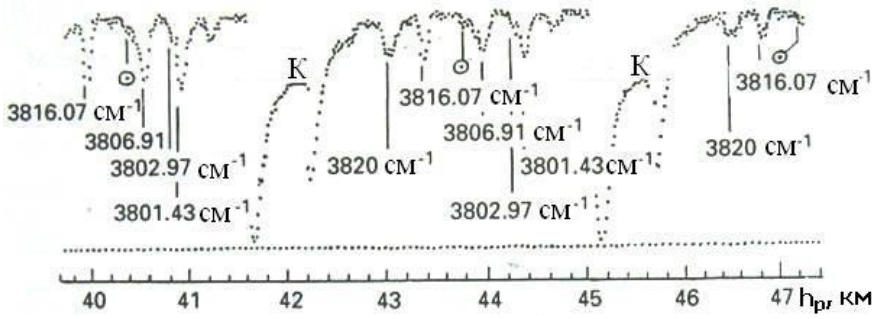


Рис. 2. Пример записи спектров поглощения солнечного излучения водяным паром в полосе 2,7 мкм на скользящих оптических трассах с помощью аппаратуры КСС-2 с пилотируемой орбитальной станции «Салют-4» при изменении высоты перигея линии визирования от 40 до 47 км (*К* – калибровочный сигнал).

При вращении космического аппарата вокруг Земли измерения проводятся на восходе и заходе Солнца. Космический аппарат за сутки делает 17 оборотов вокруг Земли, при этом спектрометр зафиксирует 34 разреза атмосферы в различных районах земного шара.

Заключение. Таким образом, за одни сутки будет получены глобальное распределение малых газовых компонентов в стратосфере и мезосфере. Последующее вращение космического аппарата позволяет получить данные о вертикальном распределении малых газовых компонентов на других участках атмосферы. Информацию о результатах затменного зондирования при пролёте над территорией России необходимо передавать на пункты приёма в реальном времени. При получении информации за пределами страны информация должна быть сохранена и передана на пункты приёма информации при пролёте над Россией или в реальном времени с использованием геостационарных ретрансляционных ИСЗ.

СПИСОК ЛИТЕРАТУРЫ

1. Кондратьев К.Я. Всемирная климатическая программа: принципиальные аспекты и перспективы осуществления // Информационный бюллетень семинара «Атмосфера–Океан–Космос» / Под ред. акад. Марчука Г.И. М.: Межд. центр НТИ ГКНТ. 1980. Вып. 1. С. 26–46.
2. Кондратьев К.Я. Слежение за параметрами климата со спутников // Труды Главной геофизической обсерватории. 1980. Вып. 488. С. 75–102.
3. Бузников А. А. Космическая спектрофотометрия природной среды с пилотируемых орбитальных станций // Оптический журнал. 2015. Т. 82. № 7. С.114–122.
4. Кондратьев К.Я., Бузников А.А., Покровский О.М. Глобальная экология: дистанционное зондирование. М.: ВИНИТИ, 1992. 308 с.
5. UARS. Upper Atmosphere Research Satellite. NASA. Washington: D. C., 1989. 28 p.

УДК 55.087, 55.083, 504.06

КОНЦЕПЦИЯ ВНУТРИЛАБОРАТОРНОГО КОНТРОЛЯ РЕЗУЛЬТАТОВ БИОТЕСТИРОВАНИЯ В ИСПЫТАТЕЛЬНЫХ ЭКОАНАЛИТИЧЕСКИХ ЛАБОРАТОРИЯХ ДЛЯ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОНТРОЛЯ ТОКСИЧНОСТИ ВОДНЫХ СРЕД

Величко Анна Николаевна
ЛОГКУ «Леноблэкоконтроль»
(Государственная инспекция экологического надзора Ленинградской области),
Россия, Санкт-Петербург, ул. Замшина, 6
e-mail: anveli@bk.ru

Аннотация. В докладе рассмотрены вопросы внутрилабораторного контроля, которые остро стоят при первичной аккредитации эколого-аналитических лабораторий и ежегодном подтверждении их компетенции.

Ключевые слова: *биотестирование; внутрилабораторный контроль; токсичность водных сред; экоаналитическая лаборатория.*

A CONCEPT OF INTRALABORATORY CONTROL OF BIOTESTING RESULTS IN ECOANALYTICAL LABORATORIES FOR ENHANCEMENT OF INFORMATION SECURITY OF CONTROL OF WATER MEDIUM TOXICITY

Velichko Anna
State Inspection of Ecological Supervision of the Leningrad Region"Lenoblecocontrol",
expert-laboratory department, chief specialist, Ph.D.
Russia, St. Petersburg, Zamshina str., 6
e-mail: anveli@bk.ru

Abstract. The report deals with the issues of intra-laboratory control, which are acute in the primary accreditation of environmental analytical laboratories and annual confirmation of their competence.

Keywords: *biotesting; intralaboratory control; toxicity of aqueous media; ecological analytical laboratory.*

Под внутренним контролем качества лаборатории подразумевают комплекс выполняемых лабораторией мероприятий и процедур, направленных на обеспечение и контроль стабильности требуемых условий для проведения исследований, а также предупреждение неблагоприятного воздействия факторов, возникающих в процессе подготовки, выполнения и оценки результатов исследований, способных повлиять на достоверность результата.

Целью внутреннего контроля качества результатов анализа является обеспечение необходимой точности результатов текущего анализа и экспериментальное подтверждение лабораторией своей технической компетентности (обеспечение точности результатов анализа не ниже гарантируемой точности методики анализа, следовательно, требуемой точности анализа).

Инструкция проведения внутрилабораторного контроля результатов биотестирования может быть разработана в соответствии с рекомендациями РМГ 76-2004, определяющей порядок и

содержание работ по внутрилабораторному контролю качества результатов количественного химического анализа при реализации в лаборатории методик с установленными показателями качества, а также в соответствии с рекомендациями ГОСТ Р ИСО 5725-6-2002 "Точность (правильность и прецизионность) методов и результатов измерений. Часть 6. Использование значений точности на практике" и токсикологических методов контроля: ПНД Ф Т 14.1:2:3:4.10-04 Т 16.1:2:2.3:3.7-04 "Методика измерений оптической плотности культуры водоросли хлорелла (Chlorella vulgaris Beijer) для определения токсичности питьевых, пресных природных и сточных вод, водных вытяжек из грунтов, почв, осадков сточных вод, отходов производства и потребления"; ПНД Ф Т 14.1:2:3:4.12-06 Т 16.1:2:2.3:3.9-06 "Методика измерений количества Daphnia magna Straus для определения токсичности питьевых, пресных природных и сточных вод, водных вытяжек из грунтов, почв, осадков сточных вод, отходов производства и потребления методов прямого счета" и ПНД Ф Т 14.1:2:3:4.2-98 "Методика определения токсичности проб природных, питьевых, хозяйственно-питьевых, хозяйственно-бытовых сточных, очищенных сточных, сточных, талых, технологических вод экспресс-методом с применением прибора серии «Биотестер»" определяет порядок и содержание работ по внутрилабораторному контролю качества результатов биотестирования при реализации в лаборатории методик с установленными показателями качества.

Контроль наличия в лаборатории условий для проведения анализа является необходимым этапом обеспечения качества результатов анализа. К таким факторам контроля относятся сроки поверки (калибровки) средств измерений; условия и сроки хранения реактивов, материалов, растворов, образцов проб, модельных токсикантов; качество дистиллированной воды и другие.

В качестве средств контроля в испытательных лабораториях для количественного химического анализа используются стандартные образцы по ГОСТ 8.315; рабочие пробы с известной добавкой определяемого компонента; рабочие пробы, разбавленные в определенном соотношении; рабочие пробы, разбавленные в определенном соотношении, с известной добавкой определяемого компонента. Контрольные процедуры для внутрилабораторного результатов биотестирования осуществляют с использованием результатов испытаний и результатов контроля качества культуры на модельных токсикантов.

За результат токсикологического анализа принимают среднее арифметическое значение результатов параллельных определений, расхождение между которыми не должно превышать абсолютного значения предела повторяемости, относительное значение которого приведено в методиках. При невыполнении условия выясняют причины появления неприемлемых результатов параллельных определений.

При невыполнении условия приемлемости результатов, полученных в условиях воспроизводимости, могут быть использованы методы оценки приемлемости результатов измерений согласно раздела 5 ГОСТ Р ИСО 5725-6.

Сходимость результатов параллельных определений индекса токсичности признают удовлетворительной, если выполняется следующее условие:

$$|T - T_{min.max}| < r,$$

где r — норматив оперативного контроля сходимости; Tmax и Tmin — максимальное и минимальное значение индекса токсичности пробы параллельных определений соответственно.

При превышении предела повторяемости необходимо дополнительно получить аналогичное количество результатов параллельных определения этой же пробы. Если при этом значение показателя повторяемости равно или меньше значения критической разности CR0,95, то в качестве окончательного результата токсикологического анализа принимают среднее арифметическое значение результатов параллельных определений. Значение критической разности CR0,95 для всех результатов параллельных определений приведены в методиках. Если значение критической разности CR0,95 превышает, то в качестве окончательного результата токсикологического анализа может быть принята медиана результатов определений.

При превышении норматива оперативного контроля сходимости эксперимент повторяют. При повторном превышении указанного норматива выясняют причины, приводящие к неудовлетворительным результатам контроля, и устраняют их. Проводят дополнительную проверку чувствительности организмов к модельным токсикантам.

Для исключения грубых ошибок рекомендуется оперативно оценивать приемлемость контроля по условию

$$|X_{к\,max} - X_{к\,min}| \le 0{,}2\,X_{ср.к.},$$

где Хк max, Хк min и Хср.к.- максимальное, минимальное и среднее значения контроля соответственно.

Внедрение методик токсикологического анализа чаще осуществляется с использованием контрольных карт Шухарта на базе результатов испытаний на модельных токсикантов для каждого определенного организма.

При подготовке данной публикации были использованы материалы, собранные в результате работы в рамках проекта "Разработка биотехнической системы для экспресс-контроля токсичности водных сред на основе тест-реакции термотаксиса P. caudatum" конкурсной программы "У.М.Н.И.К.".

СПИСОК ЛИТЕРАТУРЫ

1. Величко А.Н., Захаров И.С., Кустов Т.В., Филатов Ю.В. Биотехническая система на базе тестреакции термотаксиса Paramecium caudatum для контроля токсичности водных сред // Сборник докладов XVIII международной конференции по мягким вычислениям и измерениям (SCM'2015). – Санкт-Петербург: Изд-во СПбГЭТУ "ЛЭТИ", 2015. – С. 263-266.
2. Величко А.Н., Захаров И.С. Исследование токсичности вредных веществ, обусловленной термодиффузией в стратифицированной водной среде. // Биотехносфера. – 2014. – №5. – С.35-37.

УДК 551.593:629

ЛОКАЛЬНЫЕ ФАКТОРЫ ГЛОБАЛЬНОГО ИЗМЕНЕНИЯ КЛИМАТА (К АНАЛИЗУ СИСТЕМ АТМОСФЕРНОГО МОНИТОРИНГА В МЕГАПОЛИСАХ)

Викторов Сергей Васильевич[1], Лабзовский Лев Дмитриевич[2]
[1] Научно-исследовательский центр экологической безопасности Российской академии наук
Россия, Санкт-Петербург, Корпусная ул., 18
[2] Южный Университет Науки и технологии Китая
Китай, Шэньчжэнь, 518055
e-mail: sv1941vic@yahoo.com

Аннотация. В докладе представлены современные требования к разработке и эксплуатации сети атмосферного мониторинга, основанные на концепции системы мониторинга глобальных изменений климата. Обсуждаются различные режимы выдачи информации по отдельным параметрам атмосферы, уделено внимание некоторым аспектам информационной безопасности.

Ключевые слова: *атмосферный мониторинг; глобальные изменения климата; аспекты информационной безопасности.*

LOCAL FACTORS OF GLOBAL CLIMATE CHANGING (ANALISYS OF ATMOSPHERE MONITORING SYSTEMS IN MEGALOPOLISES)

Viktorov Sergey[1], Labzovskiy Lev[2]
[1]Scientific-Research Centre for Ecological Safety RAS
Russia, St. Petersburg, Korpusnaya str., 18
[2] South university of science and technology of China
China, Shenzhen
e-mail: sv1941vic@yahoo.com

Abstract. The paper presents some modern demands for development and exploitation of atmospheric monitoring network, based on the concept of monitoring of the global climate change. Various modes of information on several parameters of the atmosphere are discussed. Attention is paid to some aspects of information security.

Keywords: *atmospheric monitoring; global climate change; aspects of information security.*

Задачи международных программ изучения изменений глобального климата Земли потребовали нового осмысления вопросов взаимодействия локальных, региональных и глобальных исследований. Пространственно-временное распределение содержания парниковых газов и атмосферных аэрозолей носит сложный характер, и аномалии этого распределения могут быть соотнесены с расположением мегаполисов и городских агломераций. Эмиссии крупных городов, возможно, являются ключевыми факторами глобального загрязнения атмосферы. На данном этапе выяснилось, что наши знания, в особенности в области генерации парниковых газов этими объектами, оказались недостаточными.

В докладе представлены современные требования к разработке и эксплуатации сети атмосферного мониторинга, основанные на концепции системы мониторинга за глобальными изменениями климата. На примере функционирующих в штатном режиме служб контроля параметров загрязнения атмосферного воздуха в мегаполисе Шэньчжэнь (юго-восток Китая) и в мегаполисе Санкт-Петербург (северо-запад России) рассмотрены вопросы адекватности существующих служб задачам глобального мониторинга атмосферы.

Предложены рекомендации организационного и технического характера, направленные на улучшение систем мониторинга атмосферы в рассматриваемых городах для полного соответствия современным требованиям не только экологической экспертизы, но и климатологического контроля.

СПИСОК ЛИТЕРАТУРЫ

1. Величко, А. А. Эволюционная география: проблемы и решения / А. А. Величко ; отв. ред. И. И. Спасская ; Российская академия наук, Ин-т географии. — Москва : ГЕОС, 2012. — 562 с.

УДК: 004.4

МАТЕМАТИЧЕСКИЕ МОДЕЛИ АНАЛИЗА ЭФФЕКТИВНОСТИ РАБОТЫ ДОБЫВАЮЩИХ СКВАЖИН

Вирстюк Анастасия Юрьевна, Микшина Виктория Степановна, Ельмендеев Алик Питибаевич
Сургутский государственный университет
Сургут,пр. Ленина, 1, Ханты-Мансийский автономный округ
e-mails: Nastua5.1991@mail.ru, mikshinavs@gmail.com, alikelm@icloud.com

Аннотация. В статье рассмотрены существующие гидродинамические и промыслово-статистические модели, применяемые для анализа эффективности работы добывающих скважин, выделены проблемы их применения в современных условиях нефтедобычи и предложено создание адаптационных геолого-промысловых моделей, учитывающих современное состояние добывающих скважин.

Ключевые слова: *добывающие скважины; эффективность; регрессия.*

MATHEMATICAL MODELS IN THE ANALYSES OF THE EFFICIENCY WORK OF OIL WELLS

Virstyuk Anastasiya, Mikshina Viktoria
SurgutStateUniversity
e-mails: Nastua5.1991@mail.ru, mikshinavs@gmail.com

Abstract. The article deals with current hydrodynamic and industrial statistical models for analyses of the efficiency work of oil wells. Also, problems of their using in the modern oil recovery are highlighted and it is proposed the creation of adaptive geological industrial models considering the modern state of oil wells.

Keywords: *oil wells, efficiency, regression.*

Введение.Финансовая устойчивость нефтегазодобывающего предприятия в значительной степени зависит от эффективного использования фонда добывающих и нагнетательных скважин.

Для определения эффективности их работы требуется изучение большого количества показателей: дебит, приемистость, обводненность продукции и т.п. Кроме того, по мере разработки месторождений появляется потребность в анализе трудноизвлекаемых запасов нефти, запасов с высокой степенью выработанности, профиля приемистости и притока скважин и т.п., что приводит к появлению новых параметров, характеризующих работу скважин. Вследствие анализа ограниченного количества показателей и отсутствия учета новых, существующие математические модели эффективности работы скважин недостаточно адекватно описывают реальное положение дел на месторождениях.

Всвязи с этим, либо сокращается оперативность принимаемых решений по той или иной скважине, либо решение, выработанное на основании ограниченного числа показателей, является не совсем верным, что ведет не к росту, а наоборот к снижению нефтедобычи или увеличению обводненности продукции. Соответственно, создание адаптационной геолого-промысловой модели анализа эффективности работы скважин, которая будет математической основой для программного обеспечения поддержки принятия решений (с выдачей рекомендаций по каждой скважине в отдельности) является актуальной задачей, тщательная проработка которой позволит найти «индивидуальный подход» к каждой скважине.

Обзор математических моделей для оценки эффективности работы скважин. Изначально для оценки и прогнозирования показателей разработки скважин (и как следствие эффективности их работы) были созданы гидродинамические методы, которые основаны на установлении взаимосвязей между дебитом для добывающих скважин (или приемистостью для нагнетательных скважин) и определяющими их перепадами давления в пласте.

Установив на основе гидродинамических исследований фактическую зависимость дебита (приемистости) от перепадов давлений в скважинах, можно решить эти уравнения относительно искомых параметров пласта и скважин и представить полученные результаты в виде индикаторной диаграммы, на основе которой вычисляется коэффициент продуктивности (приемистости), использующийся для прогноза дебитов (приемистости) скважины.

Основы современной теории гидродинамических исследований скважин были заложены в трудах таких выдающихся ученых, как Лейбензон Л. С., Щелкачев В. Н., Маскет М., Чарный И. А. и др. Однако, применение этих методов для прогнозирования эффективности работы скважин результативно, если обводненность продукции не превышает 50%, что в современных условиях является достаточно редким явлением.

Поэтому позднее был сформулирован другой подход к анализу эффективности работы обводненных и безводных добывающих скважин – промыслово-статистические методы прогноза, применение которых очень важно особенно на поздних стадиях разработки месторождений.

На данный момент разработано более 40 промыслово-статистических методов прогноза показателей разработки. Разработанные методы описываются кривыми вытеснения – различными зависимостями между такими показателями, как: отбор нефти, воды и жидкости.

Промыслово-статистические методы прогноза получили свое развитие в трудах Назарова С.Н., Сипачева Н.В., Посевича Е.В., Максимова М.И., Пирвердяна А.М., Говоровой Г.Л. и др.

Некоторые характеристики вытеснения представлены в таблице 1.

Таблица 1

Промыслово-статистические методы прогноза активных извлекаемых запасов нефти

Модель Vн = f(Vж)	Автор (год)	Тип зависимости
$V_н = \frac{V_ж}{aV_ж + b}$	Н.В.Сипачев – Е.В.Посевич (1972)	Гиперболическая
$V_н = log_a \frac{V_ж}{b}$	Б.Ф.Сазонов (1973)	Логарифмиеская
$V_н = \frac{a}{V_ж} + b$	Г.С.Камбаров (1974)	Степенная
$V_н = \frac{a}{\sqrt{V_ж}} + b$	А.М.Пирвердян (1970)	Степенная

Любую из зависимостей можно представить в следующем виде:

$$y = a_i x + b_{i,} \quad (1)$$

где y – значение величины, откладываемой по оси ординат, выраженное в соответствующей координате рассматриваемого промыслово-статистического метода;

x – значение величины, откладываемой по оси абсцисс, выраженное в соответствующей координате рассматриваемого промыслово-статистического метода;

a_i, b_i – коэффициенты, определяемые по методу наименьших квадратов.

Промыслово-статистические методы прогноза характеризуются оперативностью (экспрессностью), простотой; основываются на минимальном количестве исходных данных. Но с другой стороны, промыслово-статистические методы характеризуются рядом отрицательных черт. Во-первых, при применении экстраполяционных методов погрешность оценки показателей разработки возрастает с ростом промежутка экстраполяции. Во-вторых, на ранних стадиях разработки методы характеризуются низкой результативностью, так как показатели разработки не обладают необходимой долей стационарности (поэтому применение кривых вытеснения обоснованно только при обводненности более 50%). В-третьих, все кривые вытеснения получены эмпирическим путем на основе обобщения промысловых данных ограниченного количества месторождений, вследствие чего они могут быть не вполне корректны для месторождений (скважин), имеющих другие особенности работы. В-четвертых, для построения аппроксимационной зависимости выбирается ограниченный прямолинейный участок кривой, но не менее 5-6 и не более 10-12 точек. И, наконец, в – пятых, объективных критериев отбора характеристик не существует, расчет ведется как минимум по 3 зависимостям, по которым коэффициент детерминации наиболее близок к 1.

Поэтому в настоящее время всё большее внимание геофизических служб обращено на адаптационные геолого-промысловые модели (АГПМ), которые могут быть подобраны для скважин с любыми характеристиками и условиями работы. Благодаря этим моделям осуществляется анализ за короткий промежуток времени (в отличие от геолого-промысловых методов), поэтому экстраполяционная ошибка не накапливается. Но следует отметить, что даже для одного и того же параметра (к примеру, для нефтедобычи) уравнение регрессии, на основе которого и строятся АГПМ, может приобретать различный вид, так как пласты и скважины имеют различные эксплуатационные характеристики – обводненность более или менее 50%, однородность или неоднородность, малая или высокая вязкость нефти и т.д.:

$$\mu_t = b_0(t) + \sum b_i(t) G_i, \quad (2)$$

$$\mu_t = b_0(t) + \sum b_i(t) G_i + k_t \mu_{t-1}, \quad (3)$$

где μ_t – текущая нефтеотдача на фиксированный момент времени;

$b_0(t)$ – значение свободного члена линейного уравнения на фиксированный момент времени;

$b_i(t)$ – значение коэффициента при i-ом геолого-физическом (технологическом) параметре на время t;

G_i – геолого-физический (технологический) параметр;

k_t – коэффициент при значении предыдущей нефтеотдачи на фиксированный момент времени;

μ_{t-1} – текущая нефтеотдача в предыдущий момент времени.

В частности, математическая модель, описываемая уравнением (2), используется для объектов, выходящих из разведки, а математическая модель, описываемая уравнением (3),

предназначена для объектов, находящихся на второй стадии разработки при обводненности продукции 50-60%.

Таким образом, адаптационные геолого-промысловые модели являются очень трудоемкими, и их применение возможно и целесообразно в рамках программных средств, благодаря которым будет проводиться предварительный анализ геолого-технических параметров скважин и подбираться необходимая модель и соответствующее ей уравнение регрессии. Кроме того, АГПМ позволяют определить зависимость одного нефтепромыслового параметра от нескольких других, что является необходимым для комплексного анализа работы скважины, в частности, для определения эффективности работы, которая для нефтяных и нагнетательных скважин может складываться из различных характеристик (к примеру, распределение закачки по пластам, профиль приемистости и т.п.), а не только на основании дебита или приемистости.

Для оценки существующих промыслово-статистических и разрабатываемых адаптационных геолого-промысловых моделей был произведен следующий анализ. Для одной и той же скважины X с определенными соотношениями Q нефти (Qн) и Q жидкости (Qжид) сначала были построены две промыслово-статистические зависимости (по Камбарову и Сазонову). Полученные результаты представлены в таблице 2.

Таблица 2

Промысловые данные и данные для промыслово-статистических зависимостей

Qн	Qжид	1/ Qжид (по Камбарову)	Прогнозные значения Qн (по Камбарову)	Ln (Qжид) (по Сазонову)	Прогнозные значения Qн (по Сазонову)
256,62	364,26	2,74	224,87	5,9	217,88
227,58	356,19	*2,81*	222,29	5,88	214,86
194,85	302,55	*3,31*	201,64	*5,71*	192,74
130,42	197,71	*5,06*	128,92	*5,29*	135,12
90,94	139,98	7,14	42,36	*4,94*	88,35
90,53	138,3	7,23	38,76	4,93	86,71
89,3	136,47	7,33	34,75	4,92	84,91

На основании данных таблицы 2 были построены графики зависимости вида Qн = f(1/Qжид) и Qн = f(ln(Qжид)). По выделенным курсивом точкам, образующим линейный участок, построен график зависимости прогнозных значений (пунктирная линия), коэффициенты которой найдены по методу наименьших квадратов. Коэффициент детерминации в обоих случаях близок к 1: для метода Камбарова = 0,96, а для метода Сазонова = 0, 97.

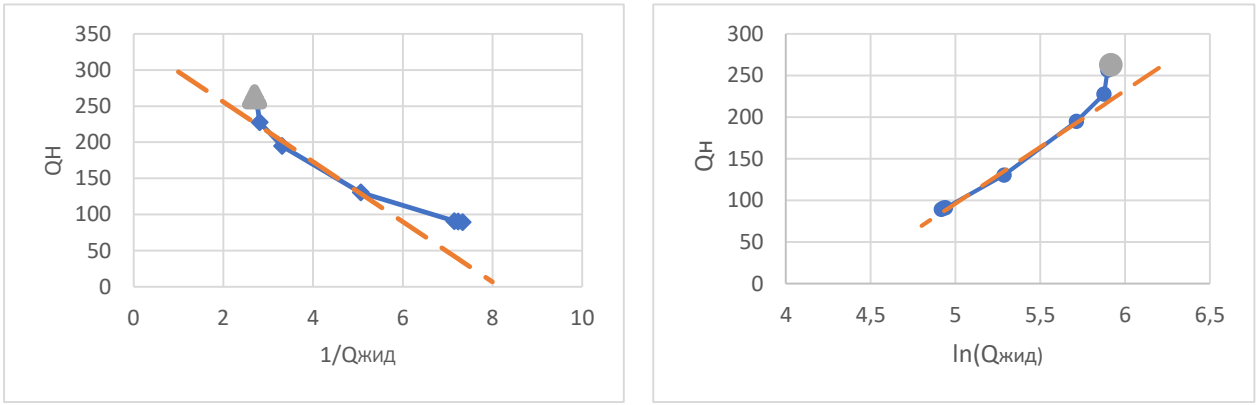


Рис. 1. Графики зависимости Qн от Qжид по методам Камбарова и Сазонова

Для анализа адекватности рассматриваемых промыслово-статистических моделей использовался F- критерий Фишера. Фактическое значение F – критерия Фишера при уровне значимости 0,05, для метода Камбарова составляет 93,6, для метода Сазонова – 201,3. F-значения уровня значимости составляют 0,0006 и 0,000007 для метода Камбарова и Сазонова соответственно, что говорит о значимости коэффициента детерминации, таким образом найденная оценка уравнения регрессии статистически надежна.

Тем не менее, в некоторых случаях данные модели не совсем адекватно оценивают реальное положение дел. Например, в соответствии с документацией по разработке месторождений Qжид в определенный момент времени достигло отметки 371 куб.м. Соответствующее ему Qн стало 262 куб.м. Но как видно из графиков (серая точка в виде треугольника и круга) по методу Камбарова при таком значении Qжид прогнозировалось Qн, равное 227 куб.м., а по методу Сазонова – 220 куб.м.

Соответственно, разные методы дали разные, хоть и близкие между собой значения, но весьма далекие от фактических, поэтому при использовании промыслово-статистических методов необходимо сравнивать между собой большее количество моделей. Но даже и в этом случае, для одних месторождений (а соответственно и скважин) модели могут подходить, а для других, с иными особенностями работы – нет.

Применение адаптационных геолого-промысловых моделей. Иная ситуация обстоит при использовании адаптационных геолого-промысловых моделей. В случае с АГПМ для анализа скважин с различными эксплуатационными характеристиками требуется разбить все исследуемые скважины на группы (провести так называемую классификацию) для того, чтобы подобрать определенный вид уравнения регрессии для каждой из них.

Для определения эффективности работы добывающей нефтяной скважины необходимо провести анализ дебита скважины и дополнительных показателей:

1) Геолого-физические: вязкость и плотность пластовой нефти, пластовая температура, содержание парафинов, пористость и проницаемость пласта, коэффициент вариации нефтенасыщенности, толщина пластов и пропластков, коэффициенты неоднородности, песчанистости и расчлененности пласта, относительные запасы нефти.

2) Технологические: темпы отбора жидкости, соотношение закачки и отбора жидкости, плотность сетки скважин и интерферирующие нагнетательные скважины, текущие запасы нефти на скважину.

Скважину X, рассматриваемую в качестве примера, можно определить к группе скважин с маловязкой нефтью и однородным объектом разработки. Вязкость пластовой нефти этой скважины составляет не более 5 МПа*с, комплексный коэффициент неоднородности не более 6. Если вязкость нефти определяется экспериментальным образом, то коэффициент неоднородности рассчитывается по формуле (4):

$$К_{неод} = \frac{W_{k1} * W_{k2}}{Mh_{эф} * Mh_{пр}}, \quad (4)$$

где Wk1, Wk2 – коэффициенты вариации, соответственно, пористости и нефтенасыщенности;

Mhэф, Mhпр – математическое ожидание, соответственно, нефтенасыщенной толщины и толщины пропластков.

Важную роль в комплексном показателе неоднородности $К_{неод}$ играет толщина пропластков. Если провести анализ $К_{неод}$при условии, что все параметры постоянные, а нефтенасыщенная толщина пропластков $Mh_{пр}$ убывает от значения $Mh_{эф}$ (пласт монолитен) до 1 м. В этом случае комплексный показатель неоднородности возрастает по гиперболическому закону, причем наиболее резко он увеличивается при уменьшении средней толщины пропластка от 5 до 1 м, что как раз соответствует интервалу, в котором наиболее сильно сказывается расчлененность пласта.

Учитывая всё вышесказанное, можно прийти к общему виду уравнения линейной регрессии для группы скважин с маловязкой нефтью и однородностью пласта:

$$E(t) = a_0(t) + a_1(t) * \mu + a_2(t) * Mh_{пр} + a_3(t) * К_{неод}, \quad (5)$$

где E(t) – эффективность работы добывающей нефтяной скважины;

$a_i(t)$ – коэффициенты;

μ - вязкость нефти;

$Mh_{пр}$ - оценка математического ожидания толщины пропластков;

$К_{неод}$ – комплексный коэффициент неоднородности пласта.

Эти показатели по скважине X представлены в таблице 3.

Таблица 3

Показатели работы скважины для уравнения множественной регрессии

Вязкость пластовой нефти, Мпа*с	Коэффициент неоднородности	Мат.ожидание толщины пропластков	Q нефти
5	5	20	90,94
2	2	21	89,301
4	6	20	90,533
1	6	15	130,419
2	5	12	194,847
5	2	9	262,902
1	1	10	256,619
2	2	11	227,583

Далее был проведен анализ по F-критерию Фишера при коэффициенте детерминации R = 0,996. Значение F-критерия Фишера равно 186,2429, а соответствующее ему значение уровня значимости равно 0,0009. Считается, если указанное значение меньше уровня значимости α = 0,05, то построенная регрессия считается значимой, что в данном случае и выполняется.

Заключение. Таким образом, на основании анализа существующих и предлагаемой моделей оценки эффективности работы добывающих скважин, относящихся к группе скважин с маловязкой нефтью и однородным пластом, адаптационная геолого-промысловая модель имеет больший коэффициент детерминации, характеризуется большей адекватностью и соответствует современным условиям процесса нефтедобычи на месторождениях.

СПИСОК ЛИТЕРАТУРЫ

1. Григулецкий В.В. Обводнение месторождений - коренной вопрос современности российской нефтегазовой отрасли [Электронный ресурс] //Технологии ТЭК. 2007 URL:http://www.oilcapital.ru/edition/technik/archives/technik/technik_02_2007/108204/public/108222.shtml (дата обращения: 29.04.2017).
2. Гамилова Д.А., Буренина И.В. Управление фондом скважин на основе комплексной оценки эффективности их эксплуатации [Электронный ресурс] // Электронный научный журнал «Нефтегазовое дело». 2007. N1. URL: http://ogbus.ru/authors/Gamilova/Gamilova_1.pdf. (дата обращения: 21.04.2017).
3. Токарев М.А., Чинаров А.С. Статистические методы прогноза нефтеотдачи и оценки эффективности воздействия на пласт: учеб.пособие. Уфа: ООО «Монография», 2007.

УДК 528.8.044.6

ДИСТАНЦИОННОЕ ЗОНДИРОВАНИЕ ПРИБРЕЖНЫХ ВОД ОХОТСКОГО МОРЯ: СРАВНЕНИЕ СПЕКТРОМЕТРИЧЕСКОГО И ЛИДАРНОГО МЕТОДОВ

Горяинов Виктор Сергеевич[1], Бузников Анатолий Алексеевич[1], Черноок Владимир Ильич[2]
[1]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
им. В.И. Ульянова (Ленина)
Россия, Санкт-Петербург, ул. Профессора Попова, 5
[2] Научно-исследовательский и проектно-конструкторский институт по развитию и эксплуатации флота «Гипрорыбфлот»
Россия, Санкт-Петербург, ул. Инструментальная, 8
e-mails: v_gor@protonmail.com, aabuznikov@mail.ru, chernook@mail.ru

Аннотация. В докладе рассматриваются два метода определения прозрачности природных вод: пассивный спектрометрический и активный, основанный на лидарном зондировании. Сравниваются результаты применения этих методов при исследовании прибрежных вод Охотского моря. Описан алгоритм оценки прозрачности воды, в основе которого лежит аппроксимация формы лидарного эхо-сигнала асимметричной гауссовой функцией.

Ключевые слова: *лидары; прозрачность природных вод; спутниковые спектрометры.*

REMOTE SENSING OF COASTAL WATERS OF THE SEA OF OKHOTSK: A COMPARISON OF SPECTROMETRIC AND LIDAR METHODS

Goryainov Viktor[1], Buznikov Anatoliy[1], Chernook Vladimir[2]
[1]St. Petersburg Electrotechnical University «LETI»
Russia, St. Petersburg, Professora Popova str., 5
[2] Research and engineering institute for the development and exploitation of fleet “Giprorybflot”
Russia, St. Petersburg, Instrumentalnaya str., 8
e-mails: v_gor@protonmail.com, aabuznikov@mail.ru, chernook@mail.ru

Abstract. The report describes two methods for assessment of turbidity of natural waters: the passive spectrometric one and the active one based on the LiDAR sounding. Results obtained using these two methods for survey of coastal waters of the Sea of Okhotsk, are compared. An algorithm for water turbidity assessment is described, based on approximation of LiDAR return shape by an asymmetric Gaussian function.

Keywords: *LiDAR; turbidity of natural waters; satellite spectrometers.*

Данные дистанционного зондирования Мирового океана находят применение во многих видах человеческой деятельности, в том числе для оценки экологического состояния и биологической продуктивности природных вод. При всем разнообразии дистанционных методов их можно разделить на две большие группы по источнику зондирующего излучения.

Пассивные методы дистанционного зондирования опираются на регистрацию солнечного излучения, рассеянного целью. К числу таких приборов относятся, например, спутниковые спектрометры. Установка на борту космических аппаратов обеспечивает им широкую полосу обзора и регулярное прохождение над исследуемым регионом. В то же время пассивные методики ограничены светлым временем суток и погодными условиями, а также регистрируют сигналы только от тонкого слоя воды вблизи поверхности.

Активные приборы дистанционного зондирования включают в свою конструкцию собственный источник излучения – например, импульсный лазер в составе лидара, что повышает их потребляемую мощность питания. С другой стороны, однако, зондирование короткими импульсами позволяет получить информацию о состоянии слоев, лежащих достаточно глубоко под поверхностью (порядка десятков метров, в зависимости от общей прозрачности воды). Кроме того, активные методы зондирования в меньшей степени зависят от фоновой освещенности.

В настоящее время лидарные системы широко применяются при исследовании природных водоемов, позволяя определять прозрачность воды, обнаруживать слои повышенного рассеяния, оценивать концентрацию фитопланктона, обнаруживать погруженные объекты и загрязнения, в том числе антропогенные.

Восстановление параметров водной среды по виду лидарного эхо-сигнала представляет достаточно сложную задачу из-за необходимости учитывать целый ряд внешних и внутренних параметров лидарной системы. В связи с этим широко распространены численные методы решения обратной задачи, основанные на различных упрощениях. Авторы доклада предлагают алгоритм оценки прозрачности воды, в основе которого лежит аппроксимация лидарного эхо-сигнала асимметричной гауссовой кривой.

Дополнительную сложность в оценку состояния природных вод дистанционными методами вносит изменчивость свойств их оптически активных компонентов. Так, например, интенсивность флуоресценции фитопланктона при лидарном зондировании может меняться в зависимости от времени года и суток, погодных условий, содержания биогенных элементов и других факторов. Как следствие, возрастает роль предварительной калибровки лидарной системы по данным измерений, выполненных другим методом (контактным или дистанционным).

В докладе приводится сравнение данных о гидрооптических характеристиках прибрежных вод Охотского моря, полученных двумя различными методами. Спектральные данные были получены при помощи спутникового спектрометра MODIS. Лидарное зондирование было проведено летом 2009 года с борта самолета вдоль побережья южной части о. Сахалин и Хабаровского края. В исследовании применялся двухканальный поляризационный лидар с длиной волны зондирующего излучения 532 нм.

СПИСОК ЛИТЕРАТУРЫ

1. Алексанин А И, С.Е. Дьяков, А.В Громов, Ю.В. Наумкин, Е.В. Фомин Обработка и использование данных полярно-орбитальных спутников FENGYUN, Материалы конф. ИКИ., том 1.- Москва. -2004. - С.66-70.

УДК 621.785

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ТОНКОПЛЕНОЧНЫХ СОЛНЕЧНЫХ МОДУЛЕЙ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

Гульков Валерий Николаевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова
Россия, Санкт-Петербург, ул. Профессора Попова, 5
e-mail: vngulkov@mail.ru

Аннотация. Для повышения эффективности работы солнечных модулей было принято решение использовать концентраторную систему в виде плоских отражателей. Исследованы основные характеристики макета солнечного модуля при различных углах раскрытия двух отражателей. В результате анализа данных наблюдений при работе станции удалось зафиксировать прирост КПД на 4,7%.

Ключевые слова: *солнечный модуль; концентраторная система; плоские отражатели; коэффициент концентрации; солнечная станция; эффективность.*

INCREASING EFFICIENCY OF THIN-FILM SOLAR MODULES TO PROVIDE INFORMATIONAL AND ECOLOGIC SAFETY

Gulkov Valeriy
St. Petersburg State Electrotechnical University «LETI»
Russia, St. Petersburg, Professor Popovstr.,5
e-mail: vngulkov@mail.ru

Abstract. Using the concentrator system comprising plain reflectors was considered to increase the efficiency of solar modules. General parameters of a solar module's model were studied at various angles of exposure between two reflectors. Analysis of data obtained during work of the station showed an increase in efficiency of 4.7%.

Keywords: *solar module; concentrator system; plain reflectors; concentration coefficient; solar station; efficiency.*

Испытания макетов тонкопленочных солнечных модулей на лабораторном стенде показали возможность увеличения эффективности их работы при использовании отражательной концентраторной системы. В процессе исследования использовалась солнечная станция, состоящая из двух последовательно включенных модулей на основе двухкаскадной тонкопленочной технологии: аморфный гидрогенизированный и микрокристаллический кремний. Площадь каждого модуля, установленного на крыше «ЛЭТИ», составляет 1,43 м2, а общая вырабатываемая мощность в максимуме может достигать 250 Вт. В процессе исследований макетов был выполнен тепловой расчет концентраторов на основе плоских зеркал, расположенных с двух сторон под определенным углом к солнечным модулям. В результате расчета получены значения предельного коэффициента К концентрации плотности падающего потока, равное 2,5-3.0. Наибольшая эффективностЬ данной системы может быть получена при расположении модулей под углом 65˚ к горизонту. В этом случае температура модулей не должна превышать 85˚С. Дальнейшее увеличение температуры поверхности может привести к изменению основных параметров модуля, таких как ток короткого замыкания и напряжение холостого хода. Однако, влияние температуры на эти величины в тонкопленочных солнечных элементах не так велико, как в случае использования монокристаллических структур. Следует отметить, что достижение больших значений коэффициента концентрации приводит к росту габаритов отражателей. Так, при K=2.5, рассчитанная площадь каждого отражающего элемента составляет 1,87 м2. При этом каждый отражатель устанавливается под углом не более 800 относительно приемной поверхности модуля. Были исследованы основные характеристик макета солнечного модуля размером 10х10 см2 при различных углах раскрытия двух отражателей.

Показно, что такое конструктивное решение, при сравнительно небольших затратах, позволяет увеличить вырабатываемую мощность солнечной станции, которая, при определенных углах установки плоскостных отражательных систем относительно плоскости солнечного модуля, может изменять эффективность преобразования от 9,2 до 13,2 %.

Очевидно, что при эксплуатации станции, оснащенной системой слежения за солнцем - солнечным трекером, который исключает затенение в утреннее и вечернее время, эффективность ее работы может быть существенно повышена. Согласно данным математического моделирования концентраторной системы, для линейного увеличения достижения коэффициента концентрации, габариты отражателей должны расти экспоненциально. Поэтому, для высоких значений плотности падающего потока следует применять многоступенчатые отражатели. Как следует из данных измерений, при наличии у солнечных модулей двух дополнительных отражателей удалось зафиксировать прирост КПД на 4,7%, по сравнению с модулями без концентраторов.

Таким образом можно заключить, что концентраторная система в виде плоских отражателей является сравнительно дешевым и эффективным способом повышения эффективности работы солнечной станции.

СПИСОК ЛИТЕРАТУРЫ

1. Бубенчиков А. А., Овсянников А. Ю., Николаев М. В., Марчинский И. Ю., Шепелев А. О. Эффективность преобразования солнечной энергии // Молодой ученый. — 2016. — №28.2. — С. 46-50.

УДК 551.501.815.003.121

МЕТОД ВОССТАНОВЛЕНИЯ ПРОФИЛЯ ВЕТРА ПО ОЦЕНКАМ ШИРИНЫ СПЕКТРА РАДИОЛОКАЦИОННОГО СИГНАЛА

Денисенков Дмитрий Анатольевич, Жуков Владимир Юрьевич, Щукин Георгий Георгиевич
Военно-космическая академия имени А.Ф.Можайского
Россия, Санкт-Петербург, ул. Красного курсанта, 16
e-mails: dimasden@yandex.ru, vuzhukov2002@list.ru,ggshchukin@mail.ru

Аннотация. В работе описывается разработанный авторами метод обнаружения и определения параметров сдвига ветра когерентным метеорологическим радиолокатором. Требуемая для этого информация извлекается из формируемых в штатном режиме работы карт пространственного распределения измеряемых параметров и не требует внесения каких-либо изменений в конструкцию радиолокатора или характеристики проводимых им обзоров.

Ключевые слова: *сдвиг ветра; ширина спектра сигнала; метеорологическая радиолокация.*

METHOD OF RESTORING THE WIND PROFILE DUE TO SPECTRE WIDTH ESTIMATION OF THE RADAR SIGNAL

Denisenkov Dmitriy, Zhukov Vladimir, Shukin Georgiy
Military Space Academy named after A. Mozhaiskiy
Russia, Saint-Petersburg, Krasniy kursant str., 16
e-mails: dimasden@yandex.ru, vuzhukov2002@list.ru, ggshchukin@mail.ru

Abstract. In the report the authors describe their method of the wind shift detection and parameters identification by coherent meteorological radar. This method allows to get the information using created in regular mode maps of the measured parameters spatial spreading and do not require to make changes in the radar construction or in scan algorithms.

Keywords: *wind shift; width of signal spectrum; meteorological radiolocation.*

Информация о вертикальном профиле ветра необходима для обеспечения безопасности летательных аппаратов. Для его оперативного определения в аэропортах и на космодромах устанавливают специальные устройства – профилометры. Как правило, их устанавливают парами, способными заменять друг друга в различных метеорологических условиях [1]. Наиболее распространено сочетание лидарного и радарного профилометров. Первый работает в условиях «чистой» атмосферы, второй – при наличии частиц (в основном, гидрометеоров) способных создавать достаточной величины отражения. Одновременно рядом, как правило, находится метеорологический радиолокатор, которому можно было бы передать функции радарного профилометра и тем сэкономить значительные средства. Однако характеристики такого радиолокатора определяются из условия выполнения им своих задач ине соответствуют требованиям, предъявляемым к профилометрам.

Основная часть. Авторами разработан метод, позволяющий извлекать информацию о вертикальном профиле ветра из данных, получаемых радиолокатором в штатном режиме работы, и не требующем внесения каких-либо изменений в конструкцию или характеристики обзоров. Исходным материалом при этом служат карты ширины спектра радиальных скоростей частиц. Появление в окружающем пространстве изменений скорости или направления ветра с высотой приводит к характерным пространственным распределениям данного параметра.

Для исследования последних была разработана модель получения радиолокатором упомянутых карт [2]. При этом окружающее пространство представлялось в виде трех слоев, характеризующихся различными параметрами: отражаемостью, вектором средней скорости и шириной спектра скоростей частиц, составляющих данный слой. В верхнем и нижнем слоях все параметры считались постоянными, в среднем же скорость и/или направление ветра изменялось с высотой по линейному закону.

Численное решение модели позволило выявить три основных варианта пространственного распределения ширины спектра сигнала, соответствующих трем возможным соотношениям линейных размеров элемента разрешения радиолокатора и толщины среднего слоя. В соответствии с тем, сколько слоев одновременно попадает внутрь элемента разрешения, они были названы трех-, двух- и однослойными.

Первый из них является основным, т.к. всегда может быть достигнут путем уменьшения угла места антенны и увеличением дальности наблюдения, и несет информацию о суммарном изменении ветра, вызванном его сдвигом по величине и по направлению. Характеризуется появлением областей аномально больших (от 6 м/с и более) значений ширины спектра, имеющих вид симметрично расположенных относительно радиолокатора двух дуг окружности.

Двухслойный вариант порождает появление на карте аномально больших значений ширины спектра в виде двух симметричных спиралей. Величина области их существования по координате азимута не превышает, как правило, 30 градусов. Между ними могут образовываться спирали малых (не более 1 м/с) значений параметра.

Для однослойной модели характерно появление на карте двух симметричных спиралей малых значений ширины спектра, существующих иногда на участках более 180 градусов по азимуту. Аномально широких спектров в данном случае не возникает.

Для получения практически значимых зависимостей величины изменения ветра с высотой и параметров пространственного распределения ширины спектра скоростей модель решалась аналитически [3]. Было показано, что при трехслойном варианте возможно определение абсолютной величины изменения вектора скорости частиц в среднем слое по всей его толщине. Для этого достаточно найти максимальноедостигнутое значение параметра в области образовавшихся их аномально больших значений, а также средние значения ширины спектра в нижнем и верхнем слоях на дальности нахождения максимального значения. Толщина слоя считается равной линейному размеру элемента разрешения на дальности, предшествующей появлению аномально больших значений параметра.

Полученных оценок вполне достаточно для решения задачи обнаружения опасного сдвига ветра, являющейся важной при обеспечении полетов авиации. Если же необходимо разделить вклады, вносимые в общее изменение скорости частиц сдвигом ветра по величине и по направлению, надо добиться появления на карте ситуации, соответствующей двух- или однослойному варианту. Достичь этого можно простым поднятием антенны.

Полученные аналитические соотношения позволяют по скорости «завития» образующихся при этом спиралей рассчитать скорость изменения с высотой направления ветра. При этом предпочтителен именно однослойный вариант, при котором вращение спирали происходит с той же

быстротой, что и вращение вектора скорости. В двухслойном же варианте спираль «завивается» примерно в четыре раза медленнее ветра.

Таким образом, доказана возможность восстановления профиля ветра по данным обзоров метеорологического радиолокатора, работающего в штатном режиме. Правильность теоретических расчетов подтверждается рядом проведенных натурных экспериментов, давших положительный результат [4].

Особая ценность полученных результатов состоит в том, что на их основе может быть построен метод восстановления профиля ветра по данным некогерентного радиолокатора, что будет объектом следующих исследований авторов.

СПИСОК ЛИТЕРАТУРЫ

1. Жуков В.Ю., Щукин Г.Г. Современные проблемы метеорологической радиолокации.// Радиотехника и электроника, 2016, т.61, № 10, с. 927–939.
2. Денисенков Д.А., Жуков В.Ю. О влиянии сдвига ветра на пространственное распределение ширины спектра радиолокационного сигнала.// Радиотехнические и телекоммуникационные системы, 2016, №1, с. 5–14.
3. Д.А.Денисенков, В.Ю.Жуков. Обнаружение сдвига ветра на основе анализа карт ширины спектра сигнала, принимаемого метеорологическим радиолокатором.//Вестник Российского нового университета., 2015, вып.2, с.10-13.
4. Денисенков Д.А., Жуков В.Ю., Сивак О.А., Щукин Г.Г. Исследование эффективности метода обнаружения сдвига ветра по оценкам ширины спектра радиолокационного сигнала // Ученые записки РГГМУ, 2016, № 42, с. 109–116.

УДК 551.501.45

ИНФОРМАЦИОННОЕ И ОПЕРАЦИОННОЕ ОБЕСПЕЧЕНИЕ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ДЕЯТЕЛЬНОСТИ СИЛОВЫХ СТРУКТУР И ОТРАСЛЕЙ ЭКОНОМИКИ РОССИИ

Доронин Александр Павлович, Щукин Георгий Георгиевич, Петроченко Вячеслав Михайлович, Козлова Наталья Александровна, Тимощук Александр Сергеевич, Шмалько Светлана Анатольевна
Военно-космическая академия имени А.Ф.Можайского
Россия, Санкт-Петербург, ул. Красного курсанта, 16
e-mail: astim2@yandex.ru

Аннотация. В статье рассматривается методический подход к проблеме обеспечения экологической безопасности деятельности силовых структур и отраслей экономики России на базе понятий информационного и операционного обеспечения. Авторами предлагаются геофизические методы и средства модифицирования окружающей среды, позволяющие устранить или в значительной мере снизить негативное влияние деятельности силовых структур и отраслей экономики России на окружающую среду.

Ключевые слова: *экологическая безопасность; окружающая среда; информационное обеспечение, операционное обеспечение.*

INFORMATION AND OPERATIONAL ENVIRONMENTAL SAFETY ACTIVITIES LAW ENFORCEMENT AGENCIES AND BRANCHES OF THE RUSSIAN ECONOMY

Doronin Aleksandr, Shchukin Georgiy, Petrochenko Vyacheslav, Kozlova Natalia, Timoshchuk Aleksandr, Shmalko Svetlana
Military - space academy named after A.F. Mozhayskiy
Russia, St. Petersburg, Krasnogo kursantastr., 16
e-mail: astim2@yandex.ru

Abstract. The article considers methodological approach to the problem of environmental safety activities of law enforcement agencies and branches of the Russian economy on the basis of the concepts of informational and operational security. The authors proposed geophysical methods and means of modifying the environment to eliminate or greatly reduce the negative impact of the activities of law enforcement agencies and branches of the Russian economy on the environment.

Keywords: *ecological safety; environment; information assurance, operational assurance.*

Введение. Негативное влияние загрязнения окружающей среды (ОС) на деятельность человека обусловливает необходимость поиска и разработки методов и средств, позволяющих устранить или в значительной мере снизить это негативное влияние. Наряду с совершенствованием технических средств сбора и обработки информации обокружающей среде, повышением качества прогнозирования опасных уровней загрязнения ОС в последние годы для этих целей предлагается использовать геофизические методы и средства модифицирования окружающей среды.

Информационное и операционное обеспечение экологической безопасности деятельности силовых структур и отраслей экономики России.

К настоящему времени установлено, что объектами модифицирования со стороны человека могут быть процессы и явления, наблюдающиеся практически во всех геосферах Земли (рис. 1) [1]. Вместе с тем, необходимо отметить, что уровень разработки методов и средств модифицирования (МОДИФ) различных геосфер далеко не одинаков и колеблется от уровня гипотез (как, например, в случае МОДИФ вулканов) до практического применения (как, например, в случае МОДИФ облаков и туманов).

Наличие в нашей стране конкретных методов и средств МОДИФ облаков и туманов (рис. 2, табл. 1) [2], а также многолетняя практика их применения для решения широкого круга прикладных задач (рис. 3) (например, регулярное рассеяние облаков над Москвой для проведения праздничных и спортивно-массовых мероприятий, тушение лесных пожаров искусственными осадками, перераспределение осадков и др.) приводят к пониманию того, что следует различать информационное и операционное обеспечение экологической безопасности (ИОЭБ и ООЭБ) (рис. 4).

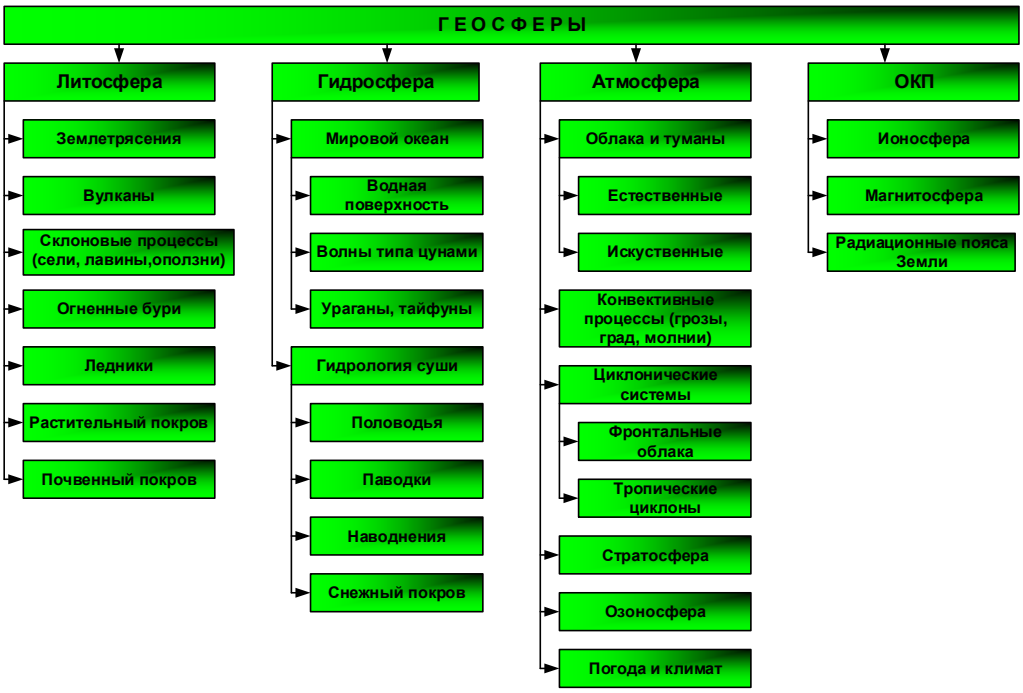


Рис. 1. Перечень геофизических процессов и явлений как возможных объектов модифицирования

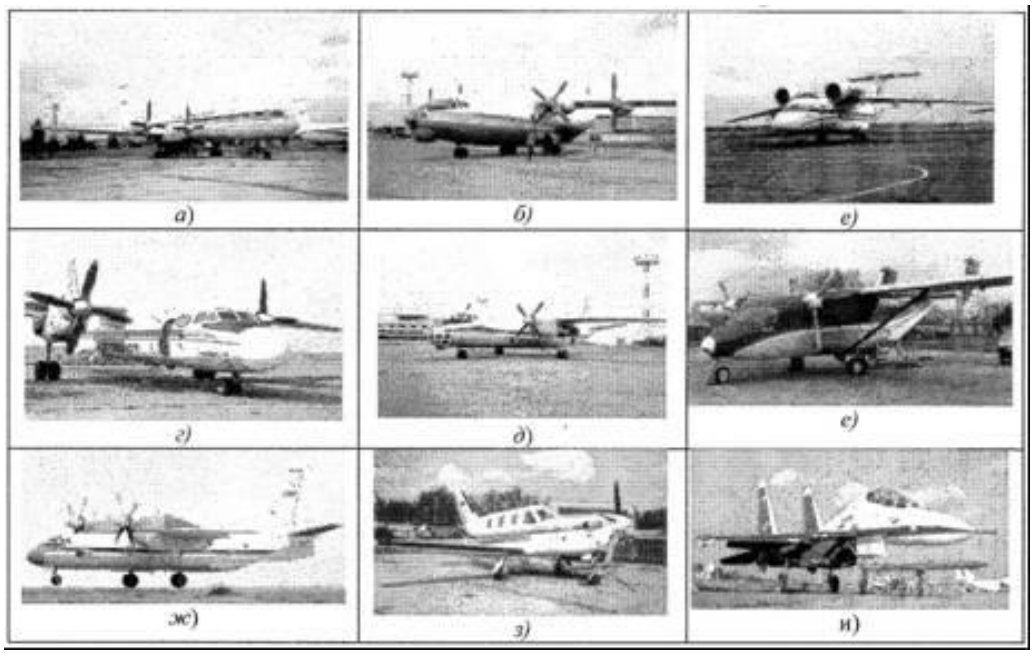


Рис. 2. Самолеты, используемые в работах по модифицированию облаков
а) Ил-18; б) Ан-12; в) Ан-72; г) Ан-26; д) Ан-30; е) Ан-28;
ж) Ан-32;з) М-101Т «Гжель»; и) СУ-30

Таблица 1

Основные характеристики самолетов, используемых в работах по модифицированию облаков

Тип сам-та / Хар-ка	Ил-18	Ан-12	Ан-72	Ан-30	Ан-32	Ан-26	Ан-28	М-101Т Гжель	СУ-30
Взлетная масса, кг	61 000	61 000	33 000	21 000	27 000	24 000	6 500	3 720	33 000
Крейсерская скорость, км/ч	617	590	550	430	530	430	337	360	360-2 200
Практический потолок, м	10 000	9 800	11 800	7 300	9 400	7 300	6 000	8 000	20 000
Максимальная дальность полета, км	4 270	4 560	4 400	2 550	2 160	2 340	1 250	1 400	3 200
Максимальная полезная нагрузка, кг	13 500	20 000	10 000	5 500	6 700	4 100	2 000	630	7 000

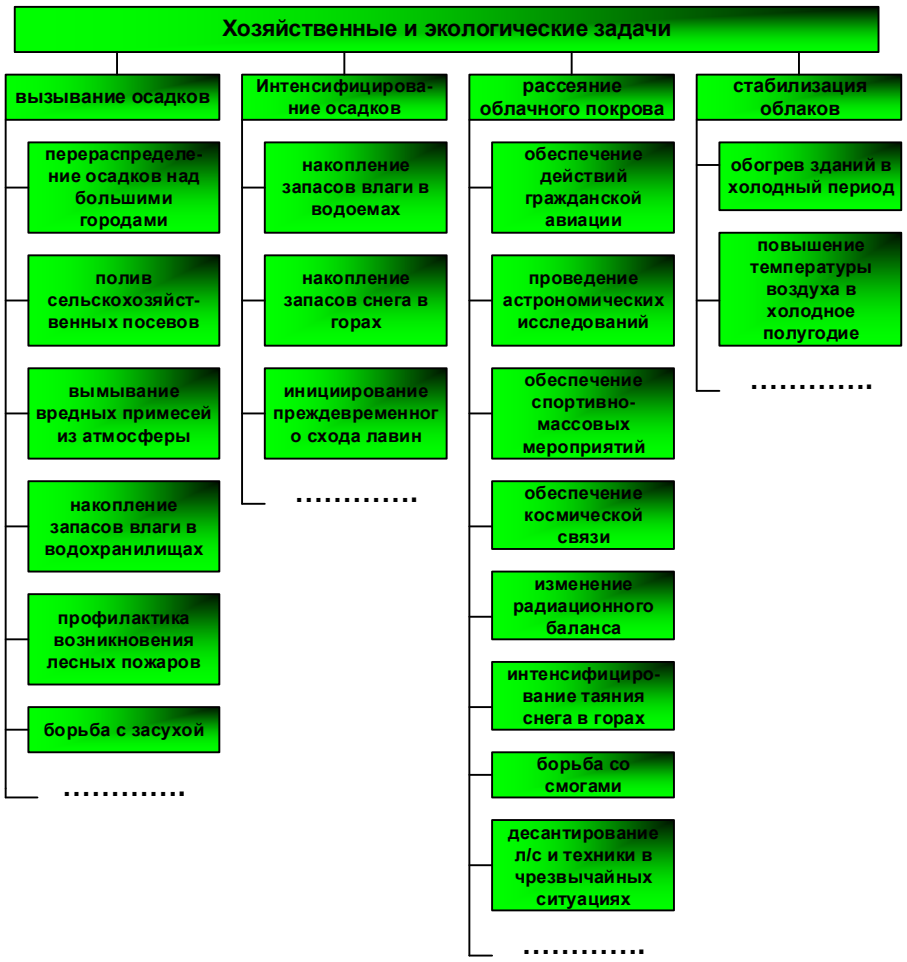


Рис. 3. Перечень прикладных задач, решаемых при модифицировании облаков

Необходимо отметить, что ИОЭБ и ООЭБ взаимосвязаны. Эта взаимосвязь проявляется в том, что для получения и переработки информации (в том числе и экологической) необходимо проводить операции (целенаправленные действия), а для организации и проведения операций необходима информация о состоянии окружающей среды. Поэтому, говоря об ООЭБ, необходимо иметь в виду потребное ИОЭБ, и, наоборот, говоря об ИОЭБ, следует иметь в виду ООЭБ.

Схематично, взаимосвязь между ООЭБ и ИОЭБ изображено на рис. 5.

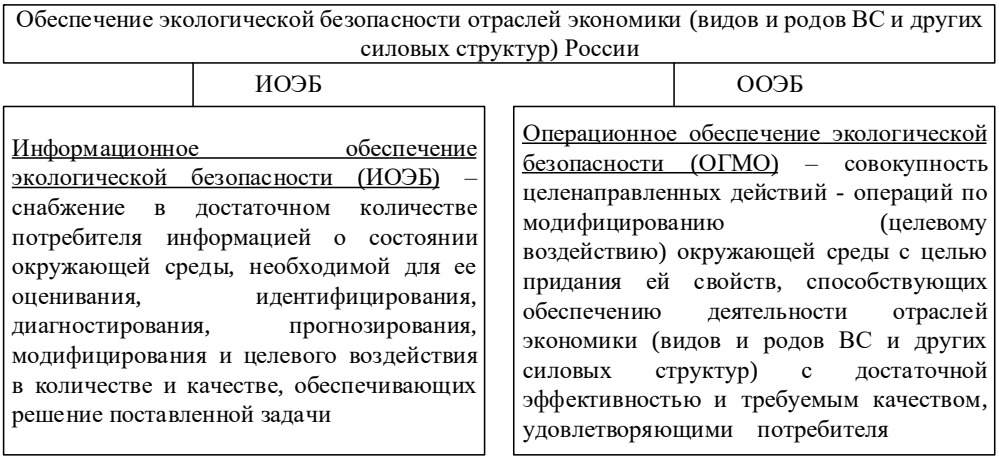


Рис.4. Информационное и операционное обеспечение экологической безопасности деятельности отраслей экономики (видов и родов ВС, других силовых структур) России

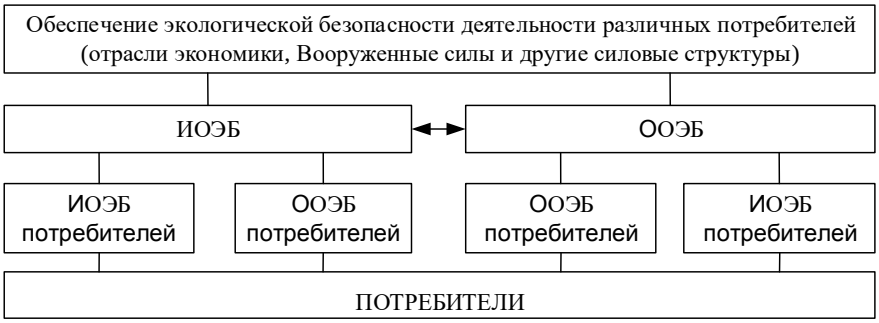


Рис.5. Взаимосвязь и совокупность ИОЭБ и ООЭБ различных потребителей

Заключение. Предложенный в настоящей работе методический подход к проблеме обеспечения экологической безопасности деятельности силовых структур и отраслей экономики России на базе понятий информационного и операционного обеспечения, по мнению авторов, позволит существенно повысить качество этого вида обеспечения, за счет оперативного внедрения в практику методов и средств модифицирования геофизических процессов и явлений и, в первую очередь, облаков и туманов.

СПИСОК ЛИТЕРАТУРЫ

1. Доронин, А.П. Состояние и перспективы работ в области модифицирования геофизических процессов и явлений в США / А.П. Доронин, Н.Г. Козлов, А.В. Костромитинов, В.В. Удриш // Сборник материалов XXIII Всероссийской межвузовской научно-технической конференции 16-18 мая 2011 года. Ч. II. – Казань, 2011. – С. 164-165.
2. Колосков Б.П., Корнеев В.П., Щукин Г.Г. Методы и средства модификации облаков, осадков и туманов. – СПб.: РГГМУ, 2012. – 343 с.

УДК: 004.78

ОСОБЕННОСТИ РЕШЕНИЯ ЗАДАЧ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ МЕГАПОЛИСА

Жигадло Валентин Эдуардович
Филиал ФГУП ЦНИИС – ЛО ЦНИИС
194223, Россия, Санкт-Петербург, ул. Варшавская, 11
e-mail: zve@mail.ru

Аннотация. В современных условиях вопросы обеспечения экологической безопасности и контроля за состоянием окружающей среды играют все более значимую роль. В докладе подробно рассматриваются некоторые инновационные разработки, направление на решение задачи обеспечения экологической безопасности мегаполиса и реализуемые в перспективных системах управления городским хозяйством, основанных на принципах «Умного Города».

Ключевые слова: *безопасный город; умный город; экологическая безопасность; информационная система.*

FEATURES OF THE SOLUTION OF PROBLEMS OF ECOLOGICAL SAFETY OF THE MEGALOPOLIS

ZhigadloValentin
Federal State Unitary Enterprise TSNIIS branch – LO TSNIIS
194223, Russia, St. Petersburg, Varshavskaya St.,11
e-mail: zve@mail.ru

Abstract. In modern conditions questions of ensuring ecological safety and control of a state of environment play more and more significant role. In the report some innovative developments, the direction on the solution of a problem of ensuring ecological safety of the megalopolis and realized in the perspective control systems of municipal economy based on the principles of "the Smart City" in detail are considered.

Keywords: *safe city; "Smart City"; ecological safety; information system; safe citymanagement of transport; information system.*

В докладе в качестве базовой рассматривается идея создания автоматизированнойсистемы регулирования транспортного потока, обеспечивающей реализацию одного из подходов к обеспечению экологической безопасности в городе.

Предполагается наличие в мегаполисе трех уровневого экологического зонирования – зеленая зона (исторический центр, центры отдыха и досуга (садово-парковые зоны) и спальные районы), желтая зона (деловые центры города) и красная зона (пригороды и промзоны). Для организации пропуска автомобилей в различные зоны (разделенные по уровню экологической безопасности) предлагается снабжать машины специальными метками со встроенными чипами, выполненными, например, по технологии RFID. Для наглядности чипы могут быть дополнены информационными наклейками-плакетками (стикерами), размещенными на лобовом стекле автомобиля. Зеленая наклейка означает, например, что можно въезжать в самый центр и спальные районы, желтая - в районы, прилегающие к центру, а красная - на "окраины" центра или исторической застройки и в промышленные зоны.

Присвоение «стикеров» для различных категорий автотранспорта может быть выполнено по следующему принципу:

– для дизельных авто (как более экологически грязных): Зеленая - на авто с Евро 4 и выше, Желтая - Евро 3, Красная - Евро 2 и ниже.

– для бензиновых: зеленая - с Евро 3 и выше, Желтая с Евро 2 и ниже.

Такое разделение авто позволяет обосновать ограничение въезда легковых и грузовых автотранспортных средств в выделенные зоны города.

В докладе подробно рассматриваются системотехнические особенности построения данной системы, возможность ее интеграции с другими системами обеспечения транспортной безопасности, а также возможности ее применения для решения других задач в рамках мегаполиса, например, организация автоматизированной оплата платных парковок.

СПИСОК ЛИТЕРАТУРЫ

1. Резолюция 4-й конференции «Система распределенных ситуационных центров − 2014», 16−17 октября, г. Воронеж.
2. Резолюция 5-й конференции «Система распределенных ситуационных центров», 7-9 октября 2015 г., г. Ярославль.

УДК 55.087, 55.083, 504.06

ПРОБЛЕМЫ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О БЕЗОПАСНОСТИ ВОДНОЙ СРЕДЫ БИОТЕСТИРОВАНИЕМ НА ОСНОВЕ СУЩЕСТВУЮЩИХ НОРМАТИВОВ

Захаров Игорь Сергеевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Россия, Санкт-Петербург, ул. Профессора Попова, 5
e-mail: Sergeich188@gmail.com

Аннотация. Рассмотрены проблемы взаимосвязи биотестирования и нормирования токсичности, на разных уровнях контроля, и последствия технические и экономические.

Ключевые слова: *биотестирование; тест-объекты; ПДК; ИЗВ; аппаратный контроль.*

PROBLEMS OF OBTAINING INFORMATION ON SAFETY OF THE WATER ENVIRONMENT BY BIOTECHING ON THE BASIS OF EXISTING REGULATIONS

Zakharov Igor
St. PetersburgState electrotechnical university “LETI”,
Russia, Saint Peterburg, Professor Popov str., 5
e-mail: Sergeich188@gmail.com

Abstract. Problems about interaction between bioassay and toxic standard for different ecology’s levels, which create technical and economic consequences.

Keywords: *bioassay; test-objects; MPC; IWP; apparatus control.*

Безопасность – важнейший информационный фактор развития человека и среды. Сегодня развиты методы биологического контроля токсичности водных сред, которые основаны на восприятии биологическими объектами интегрального загрязнения вредными веществами.

При этом тест-объекты биотеста (лабораторно полученные организмы) должны иметь чувствительность к модельным токсикантам на основе лабораторно полученных веществ. Их концентрации должны быть сравнимы с нормативами.

В докладе автором рассматриваются этапы развития нормативов в СССР, России и за рубежом, выявляются различия санитарно-гигенических и экологических норм.

Особое внимание уделяется нормативам для рыбохозяйств и трактовке информации результатов при распространении их на воду реки Невы.

Сопоставляется возможности обнаружения концентраций загрязнителей (например, меди и цинка) методами биотестирования при нормировании их в США и России, вод культурно-хозяйственного и рыбохозяйственного назначения.

Обращается внимание на использование для оценки качества среды индекса загрязнения воды – ИЗВ, который рассчитывается как сумма концентраций веществ к нормам, что может создать неверное представление об опасностях загрязнения воды.

Обсуждается о необходимости Закона об измерениях для установки нормативов, что требует учитывать точность измерения аппаратуры и разброс данных. При отсутствии учета Закона об измерениях любое неизбежное сверхмалое отклонение от норматива карается законом, что может повлечь коррупцию.

Отмечается, что биотестирование, основанное на эксперименте, всегда предполагает статистический расчет среднего информативного параметра, доверительного интервала среднего, что не учитывается при определении норматива.

Отдельной проблемой автор выделяет соотношение нормативов для питьевой воды и сточной, которые имеют обратную зависимость: питьевая вода по нормам менее чистая, чем взятая из Невы. При этом биотестирование отмечает как информацию об опасности – загрязнение питьевой воды и при этом тест-объекты не выявляют опасности от норм для рыбохозяйственного назначения. Рассматривается новый взгляд на информацию об опасности токсичности при сопоставлении биотестирования и биомаркеров.

В окончании доклада автор предлагает свою концепцию связи биотестирования и нормирования, которая позволит более эффективно выявлять информацию об опасности.

СПИСОК ЛИТЕРАТУРЫ

1. Строганов Н.С. // Методики биологических исследований по водной токсикологии. М., 1971. С. 14-68.

УДК 621.396.969

РАДИОЛОКАЦИОННЫЕ МЕТОДЫ ИЗМЕРЕНИЯ ГИДРОГРАФИЧЕСКИХ ПАРАМЕТРОВ МОРЯ

Орандаренко Елена Дмитриевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Россия, Санкт-Петербург, ул. Профессора Попова, 5
e-mail: orandarenko@jmail.com

Аннотация. В статье рассматриваются радиолокационные методы измерения гидрографических параметров моря. Приводятся предложения по практической реализации рассматриваемых методов.

Ключевые слова: *радиолокационные методы измерения; гидрографические параметры; обработка изображений.*

RADAR METHODS FOR MEASUREMENT OF HYDROGRAPHIC PARAMETERS OF SEA

Orandarenko Elena
St. Petersburg state electrotechnical University "LETI"
Russia, St. Petersburg, Professor Popov str., 5
e-mail: orandarenko@jmail.com

Abstract. The article examines radar techniques for the measurement of hydrographic parameters of seaProvides suggestions for practical implementation of these methods.

Keywords: *radar methods for measurements, hydrographic parameters.*

Введение.

В рамках проблемы исследования поверхности Земли дистанционными методами большое значение имеет исследование Мирового океана. При этом актуальными являются задачи, связанные с созданием методов и технических средств неконтактного измерения параметров морского дна. Эта информация нужна для формирования динамических карт глубин, что позволит повысить безопасность судоходства в мелководных районах акваторий. Среди существующих инструментов измерения гидрографических параметров моря можно выделить метод батиметрического контроля с помощью гидроакустического зондирование с применением гидролокаторов.

Непрерывное наблюдение за состоянием прибрежных акваторий важно, как для контроля опасных явлений, так и текущей батиметрии. Поэтому существует большая потребность в дистанционных методах контроля, позволяющих определять важнейшие гидрографические параметры с высоким пространственным разрешением.

В стратегии контроля структуры состояния прибрежной акватории должны быть синтезированы многочисленные источники данных, которые могли бы быть использованы государственными структурами для осуществления экологического контроля, предупреждения ЧС, управления движением судов, предотвращения террористических актов.

В настоящее время основным методом батиметрического контроля является гидроакустическое зондирование с применением гидролокаторов. Основным недостатком этих методов является высокая стоимость из-за больших временных объемов проведения судовых промеров, необходимых для построения и обновления батиметрических карт. Как следствие, информации, получаемой при использовании этих методов, свойственна большая инерционность. Это не позволяет адекватно оценивать морфодинамику гидрографических процессов при локальных во времени и пространстве ситуациях, связанных, например, со штормовыми явлениями, наводнениями, перемещением льда и др. Следует подчеркнуть, что в большинстве случаев эти процессы могут приводить к изменению структуры и рельефа дна [2,3].

Морская поверхность представляет собой сложный стохастический динамический процесс, который можно описать статистически. Исторически сложилось описание силы волнения через среднюю высоту волн, выражаемую в баллах. Наибольшую известность получили шкалы Дугласа и Всемирной метеорологической организации (ВМО) [1].

Радиолокационные методы оценки батиметрии

Для контроля рельефа прибрежных областей и идентификации ЧС необходимо выявлять информативные параметры. На данный момент основным методом получения данных о рельефе дна остается гидроакустический метод с использованием многолучевого эхолокатора. Несомненно, он является самым точным, однако имеет ряд недостатков, основные из которых – это значительные временные затраты на проведение судовых промеров и большая стоимость. Также существует возможность измерения состояния морской поверхности с использованием буев, что опять же является довольно затратным мероприятием, поскольку необходимо большое количество буев с помощью судна расставить и закрепить в нужных точках на исследуемой области.

Глобальный метод оценки батиметрии

Ранее делались попытки определения гидрографических параметров путем обработки последовательности изображений, полученных с помощью навигационного радара и оптических средств наблюдения, таких как текущий поверхностный вектор скорости, водная глубина, а также калиброванные полно-направленные спектры волн.

Связь между высотой ζ(θ) пространственно-временной непрерывной морской поверхности и последовательностью навигационных радарных изображений описана функцией передачи изображения ITF(Ω). Система получения последовательности изображений выдает последовательности изображений в полярных координатах I(θi,pol).

Дискретные последовательности сырых изображений преобразуются к последовательностям изображений, представленным в декартовых координатах I(θi). Для вычисления глобальных гидрографических параметров, глобальный анализ выполнен на дискретных 3-D изображениях спектров $G(\Omega_i)$ последовательности изображений. Для пространственных карт гидрографических параметров метод локального Диска реализован на дискретном комплексном 3D спектре $\hat{G}(\Omega_i)$, при этом пространственная структура последовательностей изображений сохранена благодаря информации о фазе.

Метод, используемый до настоящего времени, называемый здесь как "глобальный метод", основан на анализе яркостного спектра, вычисленного блочным модулем 3-D FFT, оперирующим с последовательностями изображений. 3-D FFT в терминах обработки изображения - глобальный оператор. При этом должны выполняться условия стационарности и однородности поля волн.

В отличие от этого метода, Диск требует только однородности в пространственном масштабе длины одной волны (локальная однородность), т.е. локальное волновое число не должно слишком сильно изменяться в этом пространственном масштабе.

Локальный метод («ДИСК») оценки батиметрии

Метод локального анализа (Диск) осуществляет анализ неоднородных последовательностей изображений динамической и дисперсионной поверхности. В отличие от глобального метода, Диск основан на следующем:

1. запоминание и сохранение комплексного спектра 3-D FFT изображения;
2. фильтрация комплексного спектра для выделения сигнальной волны на фоне шума, в отличие от глобального метода, в котором фильтруется яркостный спектр (мощности);

3. направленное и дисперсионное разделение комплексного спектра на спектральные отсчеты в 2-D плоскости волновых чисел при фиксированной частоте;

4. двумерное обратное преобразование Фурье спектральных отсчетов, замещающее комплексные однокомпонентные пространственные карты в пространственно-частотной области;

5. вычисление пространственной карты локальных волновых чисел из однокомпонентных изображений при фиксированной частоте;

6. составление 3-D спектров из однокомпонентиых локальных карт волновых чисел при фиксированной частоте;

7. вычисление пространственных карт гидрографических параметров на основе локальных 3-D спектров.

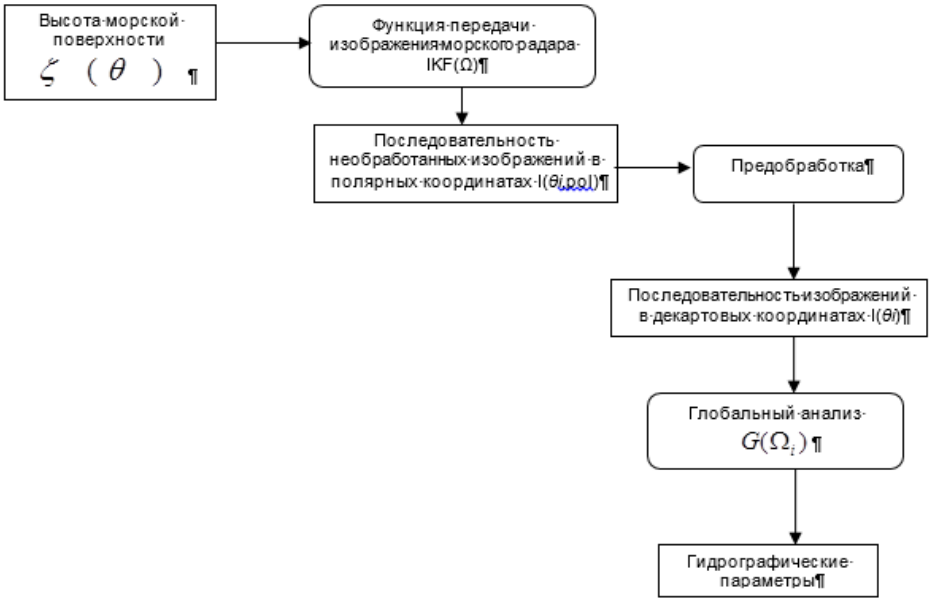


Рис.1. Принцип глобального метода

В этой работе Диск рассматривается применительно к последовательностям изображений поверхностных волн в прибрежных водах, полученным навигационными радарами. Процедура обработки и отображения последовательности изображений, получаемых Диском, проиллюстрирована на рисунке 2.

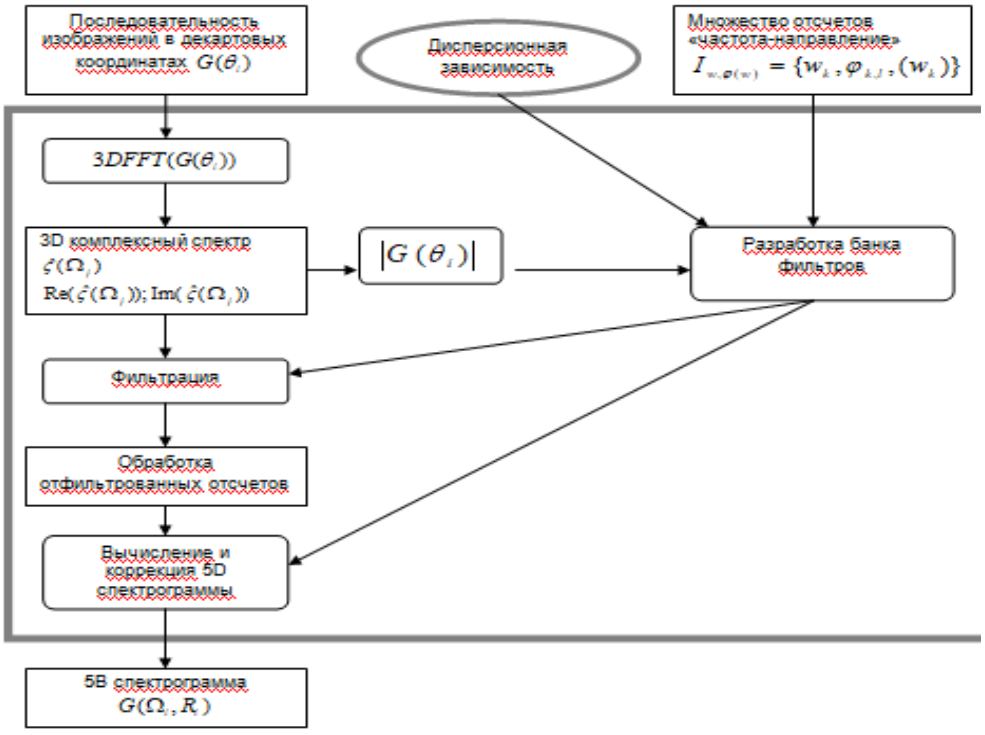


Рис. 2. Схема обработки и отображения последовательности изображений Диском

Алгоритм выдает результаты в форме пространственных карт гидрографических параметров (т. е. пространственных карт водной глубины и поверхностного течения).

В результате получаем комплексную волновую структуру, представленную в дискретах «направление-частота».

Здесь области с высокой интенсивностью волнового сигнала совпадают с пространственной когерентной фазовой структурой. Волновые векторы оценены по фазовой структуре в результате анализа по сетке квантов 16 x 16 пикселей. Заключительный шаг - построение карт текущей глубины по локальным дискретам «волновое число-частота», используя в качестве соответствующей модели дисперсионную зависимость. Пример полученной карты глубин представлен на рисунке 3 [4].

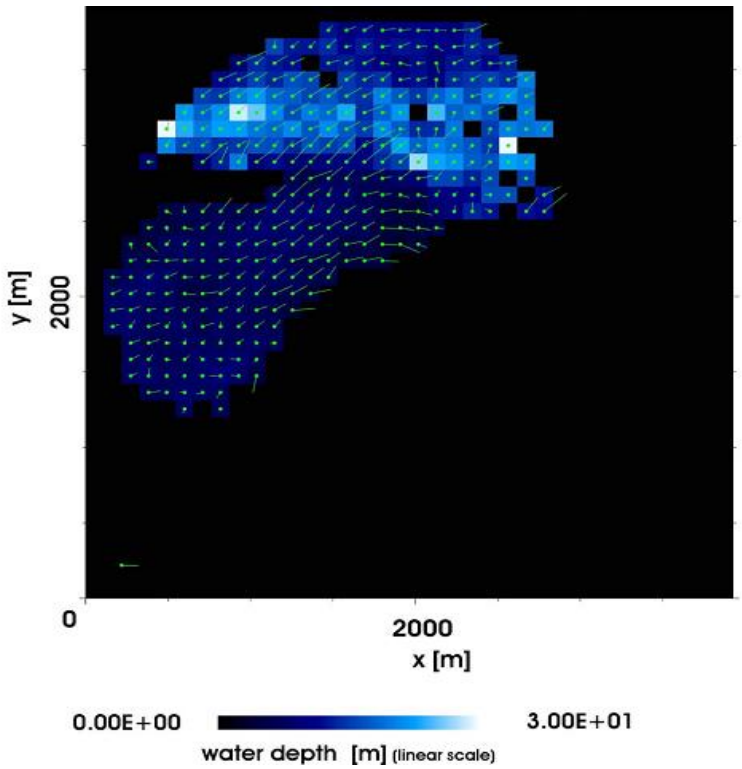


Рисунок 3. Карта батиметрии и векторов течений, определенные методом Диск по последовательности изображений, Остров Зюльт

Заключение.В статье были рассмотрены проблемы изменчивости рельефа дна. Доказательством существования проблемы служат примеры посадки на мель кораблей и судов, некоторые из которых несут за собой неприятные последствия не только для самого судна и экипажа, но также для экологии. Однако проблема имеет ряд решений, первые два из которых, гидроаккустическое зондирование и измерительные буи, трудоемки и затратны экономически. Был найден еще один метод решения проблемы – это радиолокационный метод оценки батиметрии, в котором отсутствуют недостатки предыдущих двух, и в тоже время присутствует высокая точность измерений. Данный метод получил развитие в нескольких исследовательских центрах и имеет ряд практических реализаций, те из которых рассмотрены здесь.Также информация о батиметрии и динамике её изменения, получаемая с использованием предлагаемых методов, позволят повысить безопасность судовождения в мелководных районах акваторий.

Работа была выполнена при поддержке Российского научного фонда (проект 16-19-00172).

СПИСОК ЛИТЕРАТУРЫ

1. Веремьев В. И., Коновалов А. А., Михайлов В. Н., Попов А. Г. Принципы построения многофункциональных радиолокационных комплексов мониторинга ЧС и прогнозирования состояния акваторий северных морей // XVI международная научно-техническая конференция «Радиолокация, навигация, связь», Воронеж, 13-15 апреля 2010 г. – Том 3. – С. 1744-1751
2. Hatten H., Seemann J., Senet C., Bezuglov A., Ziemer F., Veremyev V. Determination of the near surface current field from Doppler shift of the coherent radar backscatter under grazing incidence // OCEANS 2000 MTS/IEEEConference & ExhibitionProvidence, Conference Proceedings, Volume 1, pp. 549-554, Rhode Island, USA.September 11.-14., 2000.
3. Flampouris S., Ziemer F., Seeman J. Accuracy of Bathymetric Assessment by Locally Analyzing Radar Ocean Wave Imagery // IEEE TRANSACTIONS ON GEOSCIENCE AND REMOTE SENSING, VOL. 46, NO. 10, OCTOBER 2008
4. Senet C., Seemann J., Flampouris S., Ziemer F. Determination of Bathymetric and Current Maps by the Method DiSC Based on the Analysis of Nautical X-Band Radar Image Sequences of the Sea Surface (November 2007) // IEEE Trans. Geosci. Remote Sens., vol. 46, no. 8, august 2008. - C 2267-2279.

УДК 004.9

ОЦЕНКА СТРУКТУРНОЙ ЗНАЧИМОСТИ ЭЛЕМЕНТОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА

Рябовая Валентина Олеговна
Севастопольский государственный университет «СевГУ»
Россия, Севастополь, ул. Университетская, 33
e-mail: valentina_rb@mail.ru

Аннотация. В статье рассматривается метод оценки структурной значимости элементов информационной системы экологического мониторинга с учетом требований, возникших в процессе её функционирования. Определяется степень влияния каждого из элементов на функционирование системы в зависимости от функций её элементов.

Ключевые слова: *система мониторинга; системное требование; оценка значимости; функциональность.*

ESTIMATION OF STRUCTURAL MEANINGFULNESSOF ELEMENTS IS IN INFORMATIVE SYSTEMS OF ECOLOGICAL MONITORING

Ryabovaya Valentina
Севастопольский государственный университет «СевГУ»
Россия, Севастополь, ул. Университетская, 33
e-mail: valentina_rb@mail.ru

Abstract. The article considers a method for assessing the structural significance of elements of the information system of environmental monitoring, taking into account the requirements that arose in the process of its functioning. Determines the degree of influence of each of the elements on the functioning of the system, depending on the functions of its elements.

Keywords: *monitoring system; system requirement; estimation of meaningfulness; functionality.*

Введение.Использование принципов системного подхода в системах экологического мониторинга (СЭМ) — это творческий процесс. При построении функционально-эффективных вариантов СЭМ возникает задача оптимизации их структурного синтеза и исследование требует рассмотрения совокупности аспектов с учетом их взаимосвязи и использования общеизвестных системных положений [1]. Одним из главных принципов структурного анализа СЭМ является выделение наиболее существенных компонент или элементов системы с целью повышения её эффективности. Анализ литературных данных и постановка задачи**.** Анализ значимости элементов системы является традиционной составляющей при оценке её эффективности [2]. Суть анализа значимости состоит в определении степени влияния каждого из элементов системы на её функциональность. В рамках этого анализа вычисляется вероятность функционирования системы в зависимости от функций её элементов. Функционирование СЭМ — это процесс, в котором она способна реализовать заданную функцию с установленными требованиями, в течение определенного периода времени [3]. Актуальным является факт возникновения (поэтапного изменения) требований в процессе функционирования СЭМ. Предполагается, что описывающая объект структурная функция $F^S = \phi(\chi)$ является монотонной. Это объясняется тем, что при ухудшении функциональности элемента системы, значение функционирования самой системы не может возрастать [4].

Таким образом, ставится задача определения наиболее значимых элементов СЭМ, в пределах её подсистем, с учетом изменения требований в процессе функционирования.

Формализация постановки задачи и описание метода. В общем случае при исследовании целостного объекта необходима его функциональная реструктуризация на основе согласования целей (требований). При этом для одних целей оптимальные решения соответствуют минимуму значения соответствующего критерия, а для других — максимуму.

Показатели эффективности СЭМ функционально связаны с её структурой, поэтому система *S* рассматривается как кортеж, состоящий из компонент

$$S :< X, Y, F, G < D, Z >>, \quad (1)$$

где *X* — входные данные (элементы СЭМ и их функции);*Y* — выходные данные (структуры СЭМ с необходимыми функциями элементов);*F* — функциональность системы (множество функций элементов); *G* — исходная структура СЭМ;<*D, Z*>—кортеж свойств элементов СЭМ, в котором *D*— значения доминантности функциональных признаков элементов; Z — важность элементов СЭМ для Y.

Целевая функция СЭМ: $U = F_m(f_1, f_2 \dots f_n) \to \max, \quad (2)$

где *m* — число заданных для СЭМ целей, описываемых функциями f^S и f^Φ;

f^S и f^Φ — множество элементов и их функций соответственно;

$f = f^S \bigcap f^\Phi$ — функция пересечения структурно-функциональных признаков СЭМ.

Описание оптимальной структуры СЭМ в соответствии с множеством необходимых функций следующее: пусть G — исходная структура СЭМ, а G' — новая структура СЭМ, при этом:

$$G\left\{\sum_{i=1}^{k} f_i\right\} \equiv G'\left\{\sum_{j=1}^{n} f_j\right\}, \quad (3)$$

где f_i — функции исходной структуры СЭМ, f_j — функции новой структуры СЭМ, k — количество функций структуры G, n — количество функций структуры G' при $k > n$, $k < n$, и $k = n$. Подобные варианты возможны при наличии разных функциональных элементов в системе (элементов с разной функциональностью, которая и определяет эффективность работоспособности СЭМ) [5]. Для повышения эффективности данных структур каждая из них разбивается на два множества: $\{F^S\}$ и $\{F^\Phi\}$, где $\{F^S\}$ — множество элементов структуры, а $\{F^\Phi\}$ — множество функций элементов структуры.С помощью определенной замены переменных эти задачи легко сводятся к единому типу критериев и типу задач оптимизации [6]. Функция реструктуризации с учетом заданных требований:

$$F_M^R(x) = \sum_{i=1}^{m} c_i^* f^S(x) f^\Phi(x), \quad (4)$$

где c_i^*, $i = \overline{1,m}$ — коэффициенты (оценки) значимости элементов с учетом требований к СЭМ, возникших в процессе реструктуризации, f^S и f^ϕ — множество элементов и их функций соответственно.Под реструктуризацией понимается целенаправленное изменение структуры информационной СЭМ на основе элементов, формирующих её функциональность, в связи с воздействиями, оказываемыми факторами внешней или внутренней среды [7]. Определение требуемой функциональности Fx необходимого варианта СЭМ X^{F_i}, полученного методом реструктуризации, осуществляется с помощью функционального анализа и синтеза на уровне элементов системы. В данном анализе элементы рассматриваются в пределах подсистем СЭМ. Исходная структура СЭМ состоит из *n* элементов и *m* подсистем, и задана структурной функцией $\phi(x_1, x_2 ... x_n)$. Структурная функция устанавливает однозначное соответствие между возможными функциональными (работоспособными) состояниями элементов и функционирования системы [8].

Для варианта СЭМ, состоящего из *n*=7 элементов, выделяется две подсистемы *m* по $n_1 = 3$ и $n_2 = 5$ элемента в каждой. Каждая подсистема рассматривается в случае, когда её элементы имеют два варианта работоспособности (0 — при $x_i \in G'$, 1 — при $x_i \notin G'$). Структурная функция задается:

— аналитический, когда уровень функционирования подсистемы равен максимальному уровню функционирования любого из её элементов $\phi(x) = \max(x_1, x_2 ... x_n)$;

— таблично, когда структурная функция принимает значение «1», при обязательном функционировании одного или нескольких элементов.

Структурная функцияподсистемы с $n_1 = 3$ и $\phi(x) = \max(x_1, x_2, x_3)$ приведена в таблице 1.

Каждый *i*-й элемент системы характеризуется вероятностью наличия требуемой функциональности: $p(x_i) = \Pr\{x_i = s\}$, где $s = \{0,..., m-1\}$ — возможные состояния *i*-го элемента.

Таблица 1

Значение структурной функции СЭМ при $n_1 = 3$.

Элементы СЭМ и их состояния								
x_1	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_3	0	1	0	1	0	1	0	1
Структурная функция								
$\phi(x)$	0	0	0	0	0	1	1	1

Функция надежности определяется как вероятность нахождения системы в состоянии функционирования в течение заданного периода времени. Для СЭМ эта функция вычисляется как вероятность того, что в заданный временной промежуток структурная функция системы будет иметь единичное значение: $R(t) = \Pr\{T \geq t, \phi(x) = 1\}$,или в случае, когда система рассматривается в некоторый фиксированный момент, значение функции надежности определяется

$$R = \Pr\{\phi(x) = 1\}, \tag{5}$$

Значение функции неработоспособности системы:

$$F_0 = 1 - R.$$

Для анализа значимости отдельных элементов системы предлагается использовать булевы производные (булевы разности) по i-й переменной:

$$\partial\phi(x)/\partial x_i = \phi(x_1,..., x_i,..., x_n) \oplus \phi(x_1,..., \bar{x}_i,..., x_n), \tag{6}$$

где $\phi(x_1,..., x_i,..., x_n)$ — структурная функция подсистемы СЭМ, $\phi(x_1,..., \bar{x}_i,..., x_n)$ — структурная функция, в алгебраическом представлении которой переменная x_i заменяется на её отрицание $\bar{x}_i$; $\oplus$ — символ логического сложения по модулю два.

Для монотонной булевой функции, которой является структурная функция подсистемы СЭМ, имеет смысл рассматривать равнонаправленную производную вида:

$$\partial\phi(1 \to 0)/\partial x_i\,(1 \to 0) = \partial_j \phi(x)/\partial x_i.$$

Оценка структурной значимости элемента системы определяется как степень влияния исследуемого элемента с учетом топологических особенностей системы и может интерпретироваться как вероятность понижения эфективности системы при отсутствии в структурном варианте *i*-го элемента x_i .Вычисление этой оценки определяется формулой:

$$C_S(x_i) = \frac{p_i}{2^{n-1}\lambda^i}, \tag{7}$$

где p_i — число состояний системы, для которых отсутствие *i*-го элемента системы x_i приводит к понижению эффективности самой системы, λ^i — показатель требований, которые могут быть обслужены функциями элемента СЭМ.

Значение p_i определяется как число ненулевых элементов вектора значений направленной булевой производной $\partial\phi(1 \to 0)/\partial x_i\,(1 \to 0)$ структурной функции, вычисляемой по (4). Оценка структурной значимости, как правило, называется весом элемента [9].

Оценка модифицированной структурной значимости элемента определяется как вероятность неэффективной работы системы при отсутствии *i*-го элемента системы x_i

$$C_{MS}(x_i) = \frac{p_i}{p_i^{(1,1)}\lambda^i}, \tag{8}$$

где значение p_i и λ^i используются из (9), а $p_i^{(1,1)}$ — число эффективных состояний системы при наличии *i*-го элемента системы x_i: $\phi(1, x) = 1$. Эти состояния определяются на основе анализа элементов структурной функции $\phi(x)$.

При решении практических задач часто возникает ситуация, когда требуется проанализировать одновременное изменение функциональности нескольких элементов системы [10]. В этом случае оценки значимости нужно рассчитывать не для одного элемента системы, а для группы из нескольких элементов.

Структурная значимость и модифицированная структурная значимость *k*-элементов системы позволяет определить вероятность снижения уровня функционирования системы при условии снижения состояния функциональности *k*-элементов с точки зрения топологических особенностей и требований к СЭМ:

$$C_S(kx_i) = \frac{p_{ik}}{2^{n-k}\lambda^i}, \tag{9}$$

$$C_{MS}(kx_i) = \frac{p_{ik}}{p_{ik}^{(1,1)}}, \quad (10)$$

где p_{ik} — число состояний системы, для которых изменения функциональности *k*-элементов обуславливает изменение уровня функционирования системы и соответствует числу ненулевых элементов направленной булевой производной $\phi(x)$, $p_{ik}^{(1,1)}$ — число состояний системы при функционировании *k*-элементов (в таком случае имеет смысл замены двух элементов одним).

Коэффициент положительного вкладаэлемента интерпретируется как увеличение потенциала функционирования системы при использовании*i*-го элемента системы x_i.

$$C_{PW}(x_i) = \frac{\Pr\{\varphi(1_i, x) = 1\}}{R}, \quad (11)$$

где $\Pr\{\varphi(1_i, x) = 1\} = \Pr\{\varphi(x_1 ... x_n) = 1\}$ — вероятность функционирования системы, при условии использования *i*-го элемента системы X_i; *R*—значение функции надежности.

Коэффициент отрицательного вклада значимости элемента противоположен по смыслу коэффициенту $C_{PW}(x_i)$ и представляет потенциал отрицательного влияния i-го элемента системы x_i :

$$C_{NW}(x_i) = \frac{R}{\Pr\{\varphi(0,..x) = 1\}}. \quad (12)$$

Оценки структурной значимости и модифицированной структурной значимости для трех элементов СЭМ и коэффициенты положительного и отрицательного вкладов, вычисляется с использованием направленных булевых производных и приведены в таблице 2.

Таблица 2

Оценки значимости и коэффициенты вкладов элементов СЭМ

i	$C_S(x_i)$	$C_{MS}(x_i)$	$C_{PW}(x_i)$	$C_{NW}(x_i)$	*i*	$C_S(kx_i)$	$C_{MS}(kx_i)$
x_1	0.75	1	1	∞	x_1 и x_2	1	0.5
x_2	0.25	0.5	0.745	3.92	x_1 и x_3	1	0.5
x_3	0.25	0.5	0.851	6.71	x_2 и x_3	0.5	0.25

Анализ результатов таблицы 2 показывает, что обе оценки характеризуют первый элемент, имеющий максимальное влияние на функциональность системы, с точки зрения её топологических особенностей. Второй и третий элементы характеризуются одинаковым влиянием на снижение функциональности.

Представленные оценки позволяют всесторонне проанализировать влияние изменения функциональности элемента на изменение функционирования системы. Достоинство такого подхода состоит в том, что вычисление оценок значимости для одного и нескольких элементов системы осуществляется с единых методологических позиций, позволяя учитывать постоянно меняющиеся требования к СЭМ.

Заключение. Для анализа значимости элементов СЭМ, с целью определения степени влияния каждого из элементов системы на её функциональность, предложен метод оценки структурной значимости элемента системы с учетом заданных ограничений и требований к входным и выходным параметрам СЭМ, возникших до или в процессе её эксплуатации, что позволяет определить и реализовать необходимые функции.

Рассмотренные оценки значимости одного и нескольких элементов СЭМ позволяют всесторонне проанализировать влияние изменения функциональности элемента на изменение функционирования системы. Важным обстоятельством является вычисление всех оценок значимости с единых методологических позиций на основании математических методов многозначной логики и, в частности, логического дифференциального исчисления.

СПИСОК ЛИТЕРАТУРЫ

1. Imboden D., Pfenninger S. Introduction to Systems Analysis: Mathema-tically Modeling Natural Systems //Berlin, New York, Springer. — 2013. —8. — P.235-252.
2. Рябовая В.О., Доронина Ю.В. Повышение эффективности систем экологического мониторинга / В.О. Рябовая, Ю.В. Доронина // Восточно-Европейский журнал передовых технологий. — 2012. — Выпуск 4/6 (58) — Харьков: Изд-во Технологический Центр, 2012. — С. 41- 44.
3. Marek Makowski. A Structured Modeling Technology/ International Institute for Applied Systems Analysis: Laxenburg, Austria.Reprinted from European Journal of Operational Research. —2005. — 166(3). — P.615–648.
4. Zio E. Reliability engineering: Old problem and new challenges // Reliability Engineering and System Safety. — 2009. — Vol. 94.— №2.—P.125-141.

5. Barlow R., Wu A. Chogerent system with multistate elements // Mathematics of Operations Research. — 1978. — Vol.3. — № 11. — P.275-281.
6. Yau M., Apostolakis G., Guarro S. The use of prime implicants in dependability analysis of software controlled systems // Reliability Engineering & System Safety. — 1998. — Vol.62. — №1-2. — P.23-32.
7. Доронина Ю.В. Рябовая В.О. Метод структурно-функционального синтеза в задачах реструктуризации систем экологического мониторинга / Ю.В. Доронина, В.О. Рябовая // Международный научно-технический журнал «Проблемы управления и информатики». — 2013. — № 6. — С. 79-89.
8. Безопасность критических инфраструктур: математические и инженерные методы анализа обеспечения [Текст] / под ред. Харченко В.С. — Х.: Нац. аэрокосм. ун-т «ХАИ». — 2011. — 603 с.
9. Рябинин И.А., Парфенов Ю.М. Определение «веса» и «значимости» отдельных элементов при оценке надежности сложной системы // Известия АН СССР. Энергетика и транспорт. —1978. — №6. —С.22-32
10. Doronina J., Yuldasheva T. Analysis of the Integral Efficiency Indicator for Information Systems of the Cyclic Type Accounting for Weights /J. Doronina, T. Yuldasheva// Journal of Data Analysis and Information Processing. – Vol.1, Number 2, May 2013. – PP.9 –12

УДК 621.785

ГИБКИЕ ОРГАНИЧЕСКИЕ СОЛНЕЧНЫЕ ЭЛЕМЕНТЫ НА ОСНОВЕ СИСТЕМЫ «ФТАЛОЦИАНИН / ФУЛЛЕРЕН»

Тарасов Сергей Анатольевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Россия, Санкт-Петербург, ул. Профессора Попова, 5
e-mail: satarasov@mail.ru

Аннотация. В докладе рассмотрены гибкие органические солнечные элементы на основе фталоцианинов металлов, в которых достигается повышенная эффективность преобразования солнечного излучения за счет введения фуллерена.

Ключевые слова: *солнечные элементы; фталоцианины; фуллерен.*

FLEXIBLE ORGANIC SOLAR CELLS BASED ON A SYSTEM OF «PHTHALOCYANINE/FULLERENE»

Tarasov Sergey
St. Petersburg State Electrotechnical University «LETI»
Russia, St. Petersburg, Professor Popovstr., 5
e-mail: satarasov@mail.ru

Abstract. In the report presents flexible organic solar cells based on phthalocyanines of metals. The improved efficiency of created solar cells is achieved by the inserting of fullerenes.

Keywords: *solarcells; phthalocyanine; fullerene.*

Обеспечение экологической безопасности является одной из самых приоритетных задач, решаемых современной наукой. Крайне важным является контроль параметров окружающей среды для своевременного выявления природных и техногенных источников опасности. Это определяет необходимость размещения на природных территориях Российской Федерации сети климатических станций и иных датчиков, обеспечивающих непрерывный сбор данных о текущей экологической обстановке и передачу информации в режиме реального времени. Для нормального функционирования таких станций необходимо их обеспечение надежным источником электрического питания. В ряде случаев использование традиционных источников энергии оказывается затруднительным вследствие невозможности подключения указанных систем к существующим электрическим сетям, ряда существенных ограничений у существующих устройств автономного питания, а также некоторых экологических и экономических причин. В значительной степени решить указанные проблемы поможет использование для систем удаленного мониторинга устройств на основе солнечных элементов. Это позволит обеспечить бесперебойную работу климатических станций в автономном режиме, увеличить период обслуживания, и, в целом, повысить информационную безопасность системы экологического контроля.

Несмотря на значительный прогресс, достигнутый в последние годы в области создания солнечных элементов, общая стоимость солнечных модулей оказывается весьма высокой. Кроме того, во многих случаях такие системы оказываются довольно громоздкими, тяжелыми и хрупкими, что снижает их применимость в качестве автономных источников питания малоформатных удаленных систем мониторинга. Решить указанные проблемы может использование в качестве материала для солнечных элементов органических соединений различного типа. Несмотря на относительно невысокую эффективность преобразования солнечного излучения в таких элементах, их стоимость оказывается во много раз меньшей по сравнению с традиционными системами. Использование гибких пленочных подложек позволяет создавать батареи сложной формы и малого веса, что очень важно для подобных применений. В работе представлены результаты по созданию и исследованию элементов, созданных на основе низкомолекулярных и полимерных органических материалов с добавлением наночастиц.

Одними из наиболее интересных органических материалов с точки зрения их использования для создания приборов солнечной энергетики являются фталоцианины металлов. Структуры на их основе обладают высокой чувствительностью в видимой области спектрального диапазона и могут формироваться на подложках малой толщины, в том числе гибких. Были созданы и исследованы структуры на основе фталоцианина меди (FTO/CuPc/PTCDA/Al) и фталоцианина цинка, в том числе содержащих фуллерены (FTO/ZnPc:C60/C60/Al и FTO/ZnPc:C60/C60/Bphen/Al). Слои органических материалов и алюминиевый контакт наносились методом вакуумного термического испарения. Исследования показали, что спектры фоточувствительности для структур FTO/CuPc/PTCDA/Al содержит две области с высоким фотоответом: от 450 до 600 нм и от 650 нм до 1000 нм, что качественно согласуется со спектром оптического пропускания нанесенных слоев. Интересным эффектом является наличие дополнительного максимума чувствительности на длине волны 648 нм. Рассматривается его связь с диагональными переходами между уровнями HOMO и LUMO соседних фоточувствительных слоев, входящих в состав структуры.

Было подробно рассмотрено влияние введения в органические фоточувствительные структуру фуллеренов. Наиболее интересные результаты были получены для структур на основе фталоцианина цинка. Диапазон чувствительности в этом случае расширялся в длинноволновую сторону до 1150 нм. Введение в структуру FTO/ZnPc:C60/C60/Bphen/Al дополнительного транспортного слоя Bphen дало возможность понизить величины барьеров, возникающих на границе слоев и улучшить собираемость фотоносителей. В результате была получена структура, обладающая высокой чувствительностью в диапазоне 400 - 1150 нм, эффективная при использовании в качестве солнечного элемента.

Таким образом, в работе были созданы и исследованы прототипы гибких органических солнечных элементов, в которых достигается существенное увеличение эффективности преобразования солнечного излучения за счет введения в органическую матрицу включений фуллерена и оптимизации транспортных слоев в структуре. Применение таких солнечных элементов, обладающих малыми габаритами и пониженной стоимостью, в системах удаленного контроля окружающей среды должно повысить экологическую безопасность в Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. Современные фотоэлектрические и фотохимическиеметоды преобразованиясолнечной энергии / Паращук Д. Ю., Кокорин А. И. // Российский химический журнал (Журнал Рос.хим. общества им. Д.И. Менделеева). 2008. Т. LII. № 6. С. 107–117.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

УДК 004.052.2

ПРОБЛЕМА ЗАЩИТЫ ИНФОРМАЦИИ В МНОГОУРОВНЕВЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Бондаренко Игорь Борисович, Шиманчук Сергей Николаевич
Университет ИТМО
Россия, Санкт-Петербург, Кронверский пр., 49
e-mails: igorlitmo@rambler.ru, shimanchuk.s@gmail.com

Аннотация. В данной работе рассмотрены структура многоуровневых автоматизированных систем, существующие проблемы и способы их комплексной защиты, с учётом всех возможных ограничений. Для реализации защиты данных систем также были рассмотрены основы многоагентного подхода, благодаря которому, можно не просто осуществлять поиск оптимального решения на каждом уровне, но и учитывать взаимосвязи между всеми уровнями системы.

Ключевые слова: *информационные технологии; информация; многоуровневая автоматизированная система; многоуровневая система защиты; многоагентный подход.*

PROTECTION OF INFORMATION IN AUTOMATED MULTI-LEVEL SYSTEM PROBLEMS

Bondarenko Igor, Shimanchuk Sergey
St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg,Kronverksky pr.,49
e-mails: igorlitmo@rambler.ru, shimanchuk.s@gmail.com

Abstract. This paper discusses the structure of multi-level automated systems, the existing problems and their comprehensive protection, taking into account all the possible restrictions. To implement data protection systems and bases were considered multi-agent approach, thanks to which, you can't just search for the optimal solution in each level, but also take into account the relationships between all levels of the system.

Keywords: *information technology; information; multilevel automated system; multi-level protection system; multi-agent approach.*

Роль информационных технологий в современном мире невозможно переоценить. Всё, с чем имеет дело человек в любой сфере деятельности тесно связано с какой-либо техникой, на которой хранится и обрабатывается самый ценный ресурс двадцать первого века – информация.

Информация может быть не критичной, т.е. общедоступной, распространение которой обычно не влечёт за собой тяжких последствий и ущерба её владельцу, но она также может быть и конфиденциальной, распространение которой третьим лицам может привести к большим потерям.

С использованием сложных автоматизированных систем (далее АС), проблема защиты информации усложняется, так как необходимо не просто осуществление некоторой совокупности технических или организационных мер, а создание целостной системы мероприятий и применения специфических средств и методов по защите информации во всей системе.

Архитектура сложных АС представляет собой многоуровневую иерархическую систему:

1) низший уровень – это датчики и исполнительные механизмы, которые могут иметь встроенный микроконтроллер и цифровой интерфейс;

2) первый уровень составляют программируемые логические контроллеры и устройства ввода-вывода;

3) на втором уровне располагаются рабочие станции с установленными системами диспетчерского управления, которые осуществляют мониторинг и анализ действий оператора, аварийных ситуаций и запуск управляющих процедур;

4) в третьем уровне объединяются автоматизированные системы управления и автоматизированные системы управления процессами.

В зависимости от масштабов предприятия варьируется количество уровней в АС и может осуществляться интеграция с четвёртым уровнем – высшего руководства, которое может быть удалённым[1]. Более наглядно четырёхуровневая система АС представлена на «Рисунке 1».

Таким образом, необходимо обеспечить достаточную защищённость каждого уровня иерархической системы, предварительно определив все возможные актуальные угрозы перехвата информации.Для нулевого уровня актуальным будет съём информации путём использования побочных электромагнитных наводок и использование акустоэлектрического сигнала. Первый уровень необходимо защищать от съема информации по акустическому каналу, съёму информации с окон, от специальных фотоаппаратов, электросетевых подслушивающих устройств и специальных средств приёма побочных электромагнитных наводок. Со второго по четвёртый уровень к вышеперечисленным каналам утечки информации добавляются съём информации с помощью высокочастотного навязывания, с телефонной линии связи, закладных устройств и диктофонов, а также видеосъёмки[2].

Рис. 1. Многоуровневая структура АС

Кроме того, при обеспечении защиты необходимо учитывать возможные ограничения, которые могут быть габаритными, аппаратными, ограничениями по стоимости или ресурсам. Данные ограничения задаются владельцем систем исходя из целей создания системы защиты и бюджета, выделенного на создание данной системы.

Сложность решения многоуровневой защиты также заключается в том, что множество оптимальных решений, найденных на подуровнях, не означают, что достигнут оптимум для всей системы в целом. Это происходит из-за существования межуровневых связей, которые влияют на процесс нахождения решения, и приводят к тому, что сам процесс решения имеет лавинообразный характер.

В общем случае, исходя из анализа реализаций угроз на защищаемую информацию в АС, множество функций защиты выглядит следующим образом: предупреждение возникновения условий появления дестабилизирующих факторов, обнаружение появившихся дестабилизирующих факторов, предупреждение воздействий на защищаемую информацию, локализация и ликвидация последствий обнаруженного воздействия.

Если для перечисленных функций обозначить через P_r вероятность применения r-й функции при осуществлении успешной защиты, а через $P_{\text{тр}}$ – требуемый уровень защищённости информации, то можно записать следующее соотношение:

$$\mathrm{P_r} = \varphi_\mathrm{r}(\mathrm{C_r}) \geq \mathrm{P_{тр}}, \qquad \mathrm{C} = \sum_{\forall \mathrm{r}} \mathrm{C_r} \rightarrow \min, \tag{1}$$

где C_r– ресурсы, расходуемые на защиту информации.

Данное соотношение означает достижение необходимого уровня защиты при минимальных затратах на защиту информации.

Состав средств и методов, входящих в комплексную систему защиты определяется на основе проведения процедуры обследования объекта защиты, однако концепция комплексной защиты должна удовлетворять следующим требованиям:

1) использовать все механизмы защиты;

2) рационально реализовывать все необходимые мероприятия по защите информации на базе достигнутого уровня прогресса;

3) должны существовать механизмы практической реализации требуемого уровня защищённости информации[3].

Одним из решений защиты автоматизированных систем, с целью увеличения их времени функционирования является внедрение в систему блоков, которые осуществляют диагностику, реорганизацию и адаптацию структуры, подстраивая её под условия функционирования и учитывая потери от неблагоприятных воздействий. При этом работоспособные ресурсы перераспределяются и используются для достижения основной цели, но вместе с тем, отбираются у менее значимых процессов. Тем самым, количество решаемых задач уменьшается в пользу основного процесса, вследствие этого падает качество функционирования, но время функционирования растёт.

Также существует и другой подход для решения данной задачи, который заключается в выделении координирующих переменных, определяющих взаимосвязи нижних и верхних уровней. При этом необходимо декомпозировать всю систему на подсистемы с меньшей размерностью для решения локальных оптимизационных задач. После этого определяют межуровневые коэффициенты взаимосвязи и рассчитывают матрицы для коэффициентов отдельных подуровней[4].

Однако данный подход для систем с большой размерностью представляет сложную вычислительную задачу, особенно если учитывать разного рода ограничения.

В связи с этим, наиболее практичным и действующим решением для защиты сложных АС предлагается представление данных АС через многоагентную систему, которая позволяет найти оптимальное рабочее решение обеспечения безопасности на каждом уровне защищаемой АС, учитывая при этом существующие в системе межуровневые связи.

Структура такой многоагентной системы может включать в себя следующих агентов: агент-координатор уровня управления, датчиков, технологического оборудования, диспетчерского уровня, а также управляющего поискового агента. Агенты-координаторы будут являться реактивными агентами, осуществляющие распределение оптимальной защиты на каждом уровне, в соответствии с допущенными ограничениями. Взаимодействие всех агентов-координаторов осуществляется через управляющего поискового агента, на котором программируются все допущенные ограничения. Выбор оптимального рабочего решения будет осуществляться с использованием муравьиного или генетического алгоритмов, в зависимости от характеристик и размерности защищаемых АС[5].Структура разработанной многоагентной системы для многоуровневой АС представлена на «Рисунке 2».

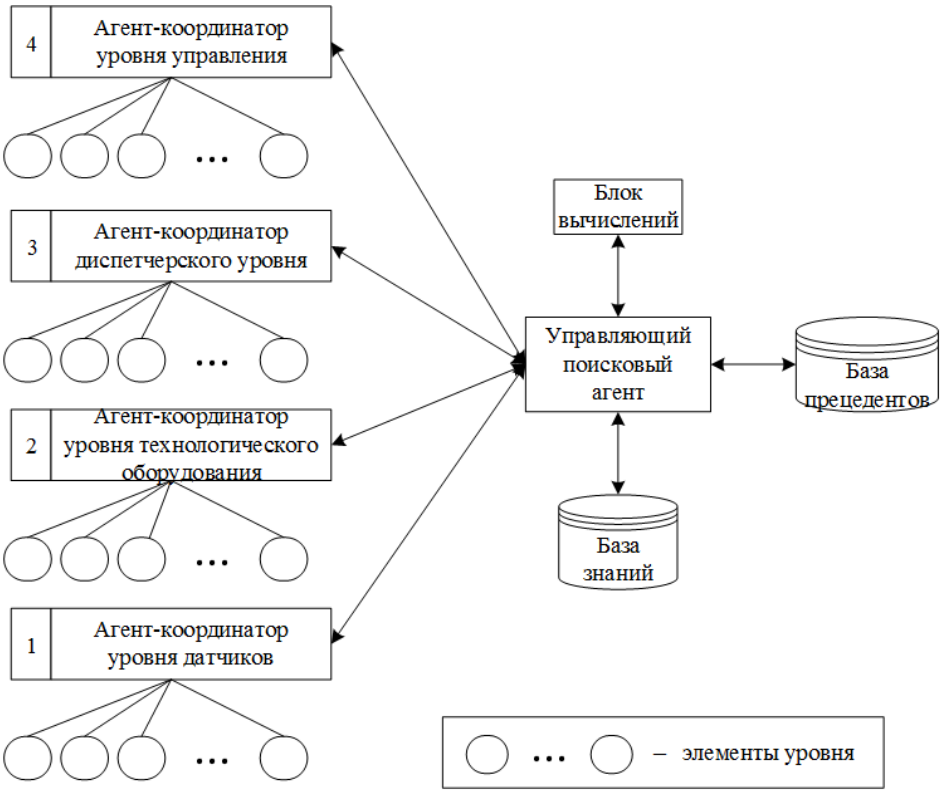


Рис. 2. Структура многоагентной системы

Заключение. Таким образом, на сегодняшний день не существует эталонной модели защиты сложных автоматизированных систем. Поэтому необходимо выстраивать свою методику защиты, объединяя несколько подходов и используя различные алгоритмы, осуществляющие поиск оптимальных решений. А также рассматривать многоуровневую АС как единую систему, чтобы

получать адекватную оценку состояния системы защиты и находить действительно оптимальное решение для всей системы в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Коробейников А.Г., Бондаренко И.Б., Прохожев Н.Н., Михайличенко О.В. Принятие технических решений с помощью многоагентных систем // NB: Кибернетика и программирование – 2013. – №1. – С. 16-20.
2. Алексенко В.Н., Древс Ю.Г. Основы построения системы защиты производственных предприятий и банков. // Учебное пособие.- М.: МИФИ, 1996.
3. Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И., Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. – М.: Гелиос АРВ,2004-265с.
4. Баранов В.В. Автоматизация управления предприятием/Баранов В.В. – М.: ИНФА-М, 2000. – 239 с.
5. Афлятунова В.А. Разработка структуры многоагентных систем для применения при расчёте нормы расхода инструмента. // Приволжский научный вестник, №1(1)/2011. С. 13–16.

УДК 004.715

АНАЛИЗ МЕТОДА БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ДЛЯ СИСТЕМЫ PAYPASS

Давыдов Вадим Валерьевич
Университет ИТМО
Россия, Санкт-Петербург, пр. Кронверкский,49
e-mail: vadimdavydov@outlook.com

Аннотация. В статье проведён обзор существующих методов аутентификации при совершении банковских платежей для карт, оснащённых технологией PayPass, а также предлагаются варианты усовершенствования безопасности при оплате такими картами путём добавления в систему оплаты метода биометрической аутентификации. Подробно рассматривается протокол PayPass, проводится анализ уязвимостей такого протокола и методы их устранения. Получен усовершенствованный протокол PayPass, в котором добавлено использование биометрической аутентификации, проведено тестирование выбранного аутентификационного метода и получены практические результаты.

Ключевые слова: *информационная безопасность; биометрическая аутентификация; бесконтактная оплата; протокол PayPass.*

ANALYSIS OF THE METHOD OF BIOMETRIC AUTHENTICATION FOR THE PAYPASS SYSTEM

Davydov Vadim
St. Petersburg National Research University of Information Technologies. Mechanics and Optics
Russia, St. Petersburg, Kronverksky pr., 49
e-mail: vadimdavydov@outlook.com

Abstract. The article provides an overview of the existing authentication methods when making bank payments for cards with PayPass technology, and also offers options for improving security when paying by adding a biometric authentication method to the payment system. The protocol PayPass is considered in detail, the vulnerability analysis of such protocol and ways of their elimination are represented. It was obtained an improved PayPass protocol with a module of biometric authentication, tested the chosen authentication method and obtained practical results.

Keywords: *information security; biometric autentification; contactless payment; the PayPass protocol.*

Введение. В настоящее время безналичный расчёт приобрёл невероятную популярность и постепенно вытесняет наличный. В частности, в России, по данным центрального банка на 2016 год, доля операций по оплате гражданами России товаров и услуг картами составила порядка 80% от общего количества транзакций, проведенных физическими лицами по своим платежным картам, что является рекордным показателем за последние пять лет [1]. Причины такой популярности кроются в удобстве и скорости платежей, а также различных бонусах за покупки, приобретённые таким способом оплаты. Начиная с 2005 года, MasterCard начала разворачивать бесконтактную технологию проведения платежей PayPass.

PayPass — это бесконтактная технология проведения платежа, основанная на стандарте ISO/IEC 14443, которая предоставляет держателям карт способ совершения оплаты путём близкого поднесения или прикосновения платёжной картой или другим платёжным инструментом, таким как телефон или брелок для ключей, к считывающему платёжному терминалу вместо вставки карты в терминал оплаты или проведения ею для считывания [2]. На сегодняшний день карты, использующие такую технологию, содержат радиочип и позволяют осуществлять бесконтактные платежи только до определённой суммы. В странах европейского союза ограничение составляет 25 евро, в США – 15 долларов, в России – 1000 рублей. Оплата при этом занимает порядка нескольких секунд.

Основная часть. Детально рассмотрим протокол PayPass. Основной задачей протокола является предоставление доказательств, что карта является подлинной и отправка на считыватель криптограммы, которая может быть отправлена в банк как доказательство проведения платежа.

На карте хранится пара открытый – закрытый ключи (PubC,PrivC) и сертификат для открытого ключа, подписанный банком, который содержит всю информацию о карте CertPrivB (PubC, Information). Карта также содержит в себе сертификат публичного ключа банка CertPrivCA (PubB), а считыватель, в свою очередь, содержит публичный ключ для сертификата PubCA. Inf – информация о банковской карте, которая представлена на карте в виде хеш-значения от всех данных карты (её номера, срока действия, имени владельца и т.д.). Для формирования криптограммы карта содержит симметричный ключ Km, который известен только карте и банку [3]. На рисунке 1 схематично изображены данные, хранящиеся на карте и считывателе.

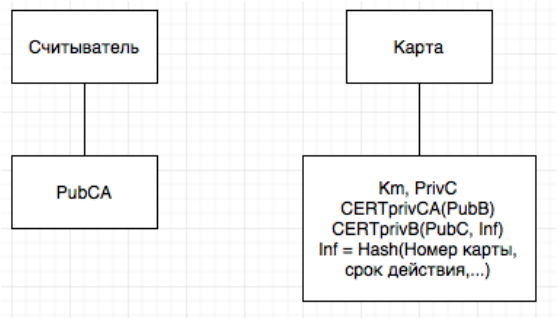


Рис. 1. Информация на считывателе и карте

В основной части протокола происходит обмен данными между картой и считывателем. Первые четыре шага иллюстрируют выбор считывателем бесконтактной технологии. Считыватель запрашивает у карты идентификаторы возможных методов (SELECT 2PAY.SYS.DDF01), в ответ карта отсылает идентификаторы с пометками систем в порядке приоритета (AID1, AID2 и так далее). После чего считыватель выбирает поддерживаемый формат с наивысшим приоритетом (SELECTPAYPASS_AID). Карта отвечает, правильно ли был выбран формат (ответ SELECTED). Далее терминал отправляет запрос на получение характеристик карты и ее специфики (GPO). В ответ карта отправляет AIP – информацию о специфике карты и AFL – данные о местонахождении информации на карте. После отправки считыватель получает все данные, напечатанные на карте (кроме CVC2 – кода на обратной стороне карточки), а также открытый ключ и сертификат, записанные на ней (READRECORD). Также считыватель получает список данных, которые он обязан предоставить карте – PAN (лицевой счёт), CDOL (информация об управлении объектами данных), после чего он имеет право составлять криптограмму в банк. На рисунке 2 показаны шаги основной части протокола – по обмену данными.

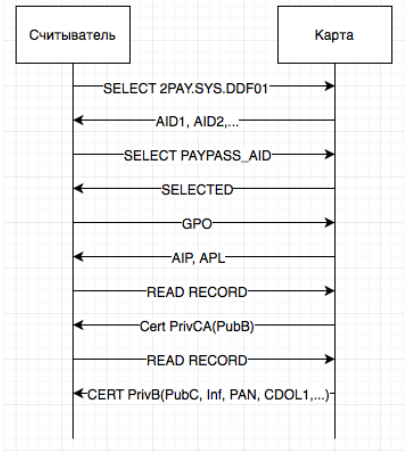


Рис. 2. Обмен информацией между картой и считывателем

В финальной части происходит проверка подлинности карты и выполнение транзакции. После получения всех данных карты считыватель генерирует одноразовый случайный код UN и запрашивает криптограмму путём выполнения команды GENERATE AC. При генерации учитываются также все данные карты. Затем карта генерирует сессионный ключ и счётчик, который равен числу раз использования карты за всё время. Этот ключ в дальнейшем используется для вычисления MAC – доказательство проведения транзакции, которое впоследствии магазин отсылает в банк. Считыватель не имеет доступа к симметричному ключу и не может проверить AC. Для предоставления доказательств, что карта подлинна, она подписывает AC вместе с одноразовым кодом и деталями транзакции – SDAD и отправляет терминалу. В свою очередь, терминал проверяет подпись и, если она верна, транзакция считается успешной.

На рисунке 3 схематично показана финальная часть протокола.

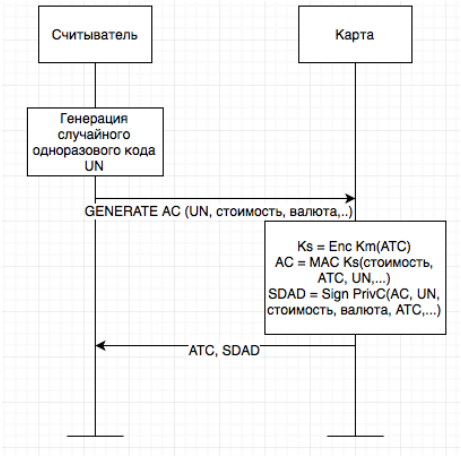


Рис. 3. Финальная часть протокола

Основной идеей внедрения такой технологии была идея сделать оплату ещё быстрее и удобнее. Однако данной технологией широко воспользовались злоумышленники. По данным компании Zecurion за 2015 год [4], мошенники украли с карт российских граждан 2 миллиона рублей. В настоящее время безопасность данной технологии ограничивается только установленным лимитом на максимальную сумму списания за один раз. При оплате с использованием такой технологии не проводится какой-либо аутентификации пользователя. Так как для проведения бесконтактных платежей требуется поднести карту к считывателю на расстояние не более 4 сантиметров [5], это даёт возможность злоумышленнику красть деньги с карты без знания об этом пользователя. В случае кражи карты злоумышленник может списывать с неё средства путём повторного снятия сумм (из-за существующего ограничения на сумму транзакции).

Ещё один тип атаки, который может быть проведён по отношению к системе PayPass, но в этом случае уже не требуется физический доступ к карте – релейная атака [6]. Схема такой атаки показана на рисунке 4.

Рис.4 Схема проведения релейной атаки

Для выполнения такой атаки противнику требуется два устройства – фейковый считыватель и фейковая карта, которые действуют в данном случае как считыватель и карта соответственно. Эти устройства подключаются друг к другу через подходящий канал связи для передачи информации на большое расстояние. Мошенник в таком случае, незаметно от жертвы, подносит к банковской карте фейковый считыватель, который, в свою очередь, передаёт информацию через канал связи на фейковую карту, а с неё информация передаётся на подлинный [7]

Приведём пример такой атаки. Мэллори хочет купить в магазине какую-то вещь, стоимость которой не превышает лимита списания по технологии PayPass. В распоряжении у Мэллори есть фейковая карта, которая подключена по каналу связи к фейковому считывателю. У него есть сообщник Ева, которая имеет при себе фейковый считыватель. Ева узнаёт, что банковская карта Алисы, оснащённая технологией PayPass, лежит у неё в заднем кармане брюк. Ева договаривается с

Мэллори, что в момент поднесения считывателя к карте Алисы Мэллори должен совершить покупку. Она подносит фейковый считыватель к карману Алисы на допустимое для проведения платежа расстояние; в этот момент Мэллори прикладывает свою фейковую карту к считывателю в магазине и совершает покупку с карты Алисы. Алиса узнаёт о том, что деньги были украдены, получив смс-оповещение от банка или посмотрев баланс в личном кабинете, но не может доказать, что это не она совершала платёж, так как при совершении транзакции не проводилось какой-либо аутентификации пользователя.

При попадании банковской карты в руки злоумышленника, он сможет совершенно свободно расплачиваться такой картой (в пределах установленного лимита) до обнаружения пользователем её отсутствия и блокировки. Чтобы предотвратить такой сценарий, целесообразно проводить аутентификацию пользователя перед совершением транзакции. Существует подобный метод оплаты посредством вставки карты в ридер и проведения парольной аутентификации, однако, основной целью разработки системы PayPass были быстрота и удобство платежа, поэтому при возможном

использовании парольной аутентификации в такой системе, она потеряет свои преимущества. Вторым вариантом аутентификации может являться ключевая система. Например, в качестве ключа может служить браслет на запястье. Если карта находится в определённом радиусе от браслета, пользователь может быть аутентифицирован. Однако такой метод влечёт за собой ряд неудобств – браслет можно забыть, потерять или сломать. К тому же, далеко не все считают удобным или эстетичным носить браслет в принципе.

Третьим вариантом является использование биометрической системы. На карту

может быть встроен биометрический сканер, который активирует радиочастотную коммуникацию между картой и считывателем только в том случае, если пользователь предъявил правильный биометрический образец системе. Данный метод не обладает недостатками предыдущих: не нужно запоминать и каждый раз вводить PIN-код, сканер, встроенный на карту, нельзя забыть или потерять. В случае потери карты, злоумышленник не сможет списывать с неё деньги, если не предоставит правильный биометрический образец. Более того, в этом случае не может быть проведена релейная атака, так как РЧ-коммуникация активируется только после прохождения аутентификации.

При выборе метода биометрической аутентификации следует руководствоваться сохранением скорости и удобства оплаты. Для этого больше всего подходит метод биометрической аутентификации по отпечатку пальца. Такой метод имеет ряд преимуществ перед остальными: он не требует дорогой аппаратуры, можно добиться высокой скорости сканирования (зависит от модели сканера), а также сам сканер обладает небольшими размерами, которые вписываются в корпус банковской карты. Однако необходимо тщательно проанализировать и оценить степень защищённости при использовании такого метода. Для этого было проведено тестирование различных современных сканеров на устойчивость к поддельным образцам. В качестве тестируемых сканеров были выбраны сканеры, встроенные на смартфоны iPhone 5s, iPhone 7 и Samsung Galaxy A5 (2016).

В процессе работы были реализованы два метода. Первый метод заключался в простом фотографировании отпечатка, его обработке, а затем печати на принтере высокого качества. Для получения отпечатка пальца использовалась камера iPhone 7. После фотографирования, изображение обрабатывалось в нескольких графических программах. Задачей было выполнить зеркальное отражение отпечатка, так как на фотографии отпечаток отражён относительно своей вертикальной оси. После такой обработки, отпечаток печатался на принтере серии Epson при максимальном качестве. Размеры напечатанного образца совпадали с размерами верхней фаланги пальца. Второй метод заключался в получении отпечатка пальца, используя такие материалы, как желатин и парафин. Для реализации такого метода были проделаны следующие действия:

1) Парафин необходимо было растопить, а затем, по мере остывания, оставить на нём образцы отпечатков пальцев.

2) Одну столовую ложку желатина необходимо смешать со стаканом воды, довести смесь до кипения и оставить на некоторое время остывать. В полученной смеси появлялись пузырьки воздуха, которые необходимо было ликвидировать – для этого несколько раз такая смесь разогревалась в микроволновке в течение 1 минуты и остывала. После 4 таких циклов пузырьков в смеси не осталось.

3) Для получения фейкового образца, лунки на парафине заливались желатином и были охлаждены. После чего аккуратно были сняты кусочки застывшего желатина, на которых получились отпечатки пальцев. В итоге получились небольшие кусочки желатина, которые можно одевать на

пальцы и тестировать на различных типах сканеров.

По итогам тестирования были получены следующие результаты:

1) Ни один из тестируемых сканеров не реагировал на изображение, напечатанное на обычном принтере.

2) Сканеры компании Apple принимали образец из желатина за реальный палец, в то время как сканер Samsung никак не реагировал на данные образцы.

3) Удалось войти в систему телефонов iPhone 5s и iPhone 7 с помощью фейкового образца, в систему смартфона компании Samsung войти не удалось.

4) Сканеры устройств Apple в большинстве случаев не распознавали фейковый отпечаток как настоящий, однако, в ограниченном числе случаев телефон был разблокирован таким способом.

Исходя из полученных результатов, можно сделать следующие выводы:

1) Биометрический сканер компании Samsung продемонстрировал устойчивость к фейковым образцам, полученным продемонстрированными выше методами.

2) Биометрические сканеры Apple в моделях iPhone имеют устойчивость к атакам путём предоставления 2D-образца, но не защищены от атак, в которых используются высокоточные 3D-модели пальцев с отпечатками.

Заключение.На основании проделанных экспериментов стало понятно, что сканеры, установленные в смартфонах Samsung Galaxy A5 «умеют» отличать настоящие пальцы от поддельных образцов, что говорит о том, что они используют специальные технологии для анализа свойств кожи. Это очень важный фактор надёжности в современных системах, так как, «обмануть» биометрический сканер можно даже в домашних условиях без использования какой-либо

специальной техники. В дальнейшем планируется выяснить, какие именно технологии использованы и применить их для создания банковской карты с встроенным сканером отпечатков пальцев. Планируется, что на карте будут записаны различные отпечатки, и по ним будет проведено разграничение доступа к средствам. На практике такая технология видится очень удобной и перспективной – к примеру, родитель может дать своему ребёнку банковскую карту, но установит лимит на списание средств. В рамках проведённых исследований важно отметить, что при выборе сканера стоит обратить самое пристальное внимание на то, каким образом работает сканер и какие типы атак возможны на систему аутентификации, так как речь идёт о благосостоянии и благополучии людей.

СПИСОК ЛИТЕРАТУРЫ

1. Россияне стали чаще оплачивать товары и услуги в магазинах картами// URL: https://www.vedomosti.ru/finance/articles/2017/03/14/681000-oplachivat-kartami (дата обращения: 23.08.17).
2. Bradford T. et al. Contactless: the next payment wave? //Payment System Research Briefing. – 2005.
3. Chothia T. et al. Relay cost bounding for contactless EMV payments //International Conference on Financial Cryptography and Data Security. – Springer Berlin Heidelberg, 2015. – С. 189-206.
4. Россияне всё больше теряют из-за краж с карт "по воздуху" // ИЗВЕСТИЯ URL: http://izvestia.ru/news/613206 (дата обращения: 23.08.17).
5. Worldwide M. C. MasterCard® PayPass (TM).
6. Markantonakis K. et al. Practical relay attack on contactless transactions by using nfc mobile phones //Radio Frequency Identification System Security: RFIDsec. – 2012. – Т. 12. – С. 21.
7. Hancke G. P. A practical relay attack on ISO 14443 proximity cards //Technical report, University of Cambridge Computer Laboratory. – 2005. – Т. 59. – С. 382-385.

УДК 004.56

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КИБЕРУСТОЙЧИВОСТЬ ЦИФРОВОЙ ЭКОНОМИКИ И ЦИФРОВОГО ПРОИЗВОДСТВА

Зегжда Петр Дмитриевич, Зегжда Дмитрий Петрович
Санкт-Петербургский политехнический университетПетра Великого
Россия, Санкт-Петербург, ул. Политехническая, 29
e-mails: kafedra@ibks.spbstu.ru, dmitry@ibks.ftk.spbstu.ru

Аннотация. В докладе исследуется вопрос киберустойчивости информационной и физической составляющей цифровых систем к кибератакам с учетом их взаимовлияния, свойств масштабируемости, интероперабельности, модульности на основе кросскорреляционных связей и оценки самоподобия и динамической устойчивости. Проведена оценка влияния кибератак на систему управления киберфизических систем с учетом адаптивности и способности к саморегуляции на основе фрактальных показателей устойчивости и способности к гомеостазу.

Ключевые слова: *киберустойчивость; кибератаки; киберфизические системы; показатели устойчивости; гомеостаз.*

INFORMATION SECURITY AND CYBER-STABILITY OF THE DIGITAL ECONOMY AND DIGITAL PRODUCTION

Zegzhda Peter, Zegzhda Dmitry
[1]Peter the Great St. Petersburg Polytechnic University
Russia, St. Petersburg, Polytechnicheskaya str., 29
e-mails: kafedra@ibks.spbstu.ru, dmitry@ibks.ftk.spbstu.ru

Abstract. In the report presents the issue of cyber-stability of computer and physical components of digital production systems to cyberattacks, their mutual influence, scalability, interoperability, modularity based on cross-correlation relationships, self-similarity and dynamic stability. Authors describe the possible damage caused by cyber attacks on the cyberphysical systems, taking into account their adaptability and self-regulation ability on the basis of fractal stability indicators and the ability to homeostasis.

Keywords: *cybersecurity; cyber-stability; cyber attacks; cyber-physical systems; homeostasis.*

Современный уровень технологического развития общества характеризуется переходом к цифровой экономике, основу которой составляют цифровое производство, «умные» вещи, интеллектуальные системы, реализующие технологические и бизнес процессы автономно от человека. Одновременно, в связи с развитием промышленной автоматизации и применением информационных технологий и интеллектуальных систем в различных областях промышленного производства, энергетики и транспорта, компьютерные системы все больше используются для управления физическими процессами и преобразуются в киберфизические системы [1].

В этих условиях получение несанкционированного доступа к информации и деструктивное кибервоздействие на компьютерные системы численного моделирования, визуализации, инженерного

анализа, разработки конструкций и автоматизированные технологические процессы приводят к гораздо более тяжелым последствиям, чем в доцифровую эпоху.

Цифровая экономика должна успешно противостоять многочисленным и разнообразным угрозам безопасности, действующим в современном киберпространстве, и главным образом тем, которые носят целенаправленный характер.

В цифровую эпоху для решения проблемы информационной безопасности недостаточно удовлетворить требования регуляторов по соблюдению конфиденциальности, целостности и доступности обрабатываемой информации, необходимо обеспечить устойчивость функционирования системы в условиях воздействия целенаправленных киберугроз -- т.н. киберустойчивость [2,3,4].

При решении задачи защиты цифровой экономики и цифрового производства от киберугроз необходимо учитывать, что основное отличие этих систем от традиционных средств обработки информации состоит в том, что их функционирование напрямую связано с физическими или бизнес процессами, которые в большинстве своем, в отличие от процессов обработки информации, являются необратимыми.

Специфика защиты цифрового производства от информационных угроз состоит в том, что основной целью является сохранение устойчивости физических процессов и непрерывности управления в условиях целенаправленных киберугроз, воздействующих на информационные компоненты [5].

Перечисленные факторы обуславливают необходимость расширения традиционных показателей информационной безопасности применительно к цифровой экономике и производству и служат основой для новых подходов и моделей обеспечения информационной безопасности в современном киберпространстве.

В докладе исследуется вопрос киберустойчивости информационной и физической составляющей цифровых систем к кибератакам с учетом их взаимовлияния, свойств масштабируемости, интероперабельности, модульности на основе кросскорреляционных связей и оценки самоподобия и динамической устойчивости.

Проведена оценка влияния кибератак на систему управления киберфизических системс учетом адаптивности и способности к саморегуляции на основе фрактальных показателей устойчивости и способности к гомеостазу.

СПИСОК ЛИТЕРАТУРЫ

1. Zanero, S. Cyber-Physical Systems // Computer Volume 50, Issue 4, 2017, Article number 7912263, Pages 14-16
2. Schneider, FB. Enforceable security policies. // ACM Transactions on Information and System Security. 2000; 3(1):30–50. DOI: 10.1145/353323.353382
3. Mulligan, D.K., Schneider, F.B. Doctrine for cybersecurity // Daedalus Volume 140, Issue 4, 2011, Pages 70-92
4. Ashibani, Y., Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions // Computers and Security Volume 68, 1 July 2017, Pages 81-97
5. ГОСТ Р ИСО/МЭК 27032-2012. «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности».

УДК 004.056

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. ФИШИНГ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ЕМУ

Ильченко Лидия Михайловна[1], Уваров Роман Валерьевич[1], Зайцев Святослав Игоревич[2]
[1] Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
[2]Государственный университет морского и речного флота имени адмирала С.О. Макарова
Российская Федерация, Санкт-Петербург, ул. Двинская, 5/7
e-mails: Lidiya9510@yandex.ru, Sunilink@yandex.ru

Аннотация. В данной работе рассматриваются такие методы социальной инженерии, как фишинг, вишинг и спуфинг, а также методы противодействия им.

Ключевые слова: *социальная инженерия; фишинг; спуфинг;TCP/IP; UDP вишинг.*

SOCIAL ENGINEERING. PHISHING AND METHODS OF COUNTERING IT

Ilchenko Lydia[1], Uvarov Roman[1], Zaytsev Svyatoslav[2]
[1]St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverkskypr., 49
[2]Admiral Makarov State University of Maritime and Inland Shipping
Russia, St. Petersburg, Dvinskaya str., 5/7
e-mails: Lidiya9510@yandex.ru,Sunilink@yandex.ru

Abstract. In this paper we consider such methods of social engineering as phishing, wishing and spoofing, as well as methods of countering them.

Keywords: *social engineering; phishing; spoofing; TCP / IP; UDP vishing.*

Введение. Существует множество векторов потенциальной атаки, рассматриваемых в рамках информационной безопасности, среди них особую популярность имеют технические каналы утечки информации: вибро-акустические, акустоэлектрические, оптические каналы, утечки по каналам ПЭМИН и др. [1]. В связи с чем постоянно развиваются средства противодействия потенциальным атакам. На сегодняшний день, обойти средства криптографической защиты информации, безупречные протоколы безопасности, средства физической защиты и пр. фактически невозможно, однако, руководители и специалисты по защите информации часто пренебрегают угрозами со стороны инсайдеров [2].

Если верить статистике, число утечек информации ограниченного доступа по вине внутреннего нарушителя в 2016 году уменьшилось по сравнению с 2015 и 2014 и составляет 61,8%, однако, это говорит о том, что на долю утечек по вине персонала все еще приходится более половины всех инцидентов. В России эта цифра более внушительная и составляет 86,7% от общей доли утечек на 2016 год. Визуально данные представлены на рисунке 1.

Данные статистических исследований говорят о низком уровне культуры информационной безопасности в нашей стране. То есть сотрудники, имеющие доступ к конфиденциальным данным, имеют свойство «забывать», что результаты их работы, а также данные, к которым они имеют доступ в соответствии со своими должностными обязанностями, являются информацией ограниченного доступа целиком и полностью принадлежат работодателю. Другой стороной данной проблемы является злоупотребление сотрудниками доступом к имеющимся у них сведениям, в том числе к персональным данным клиентов и контрагентов работодателя [3].

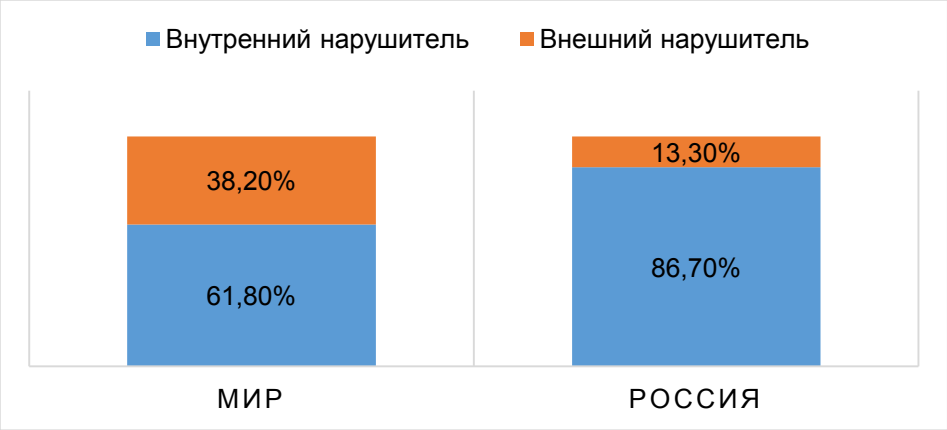


Рис. 2 Распределение утечек информации Россия – Мир.

Действия внутреннего злоумышленника можно разделить на умышленные и неумышленные действия, имеющие негативный характер.

Доля утечек информации по вине сотрудников сокращается в течение последних четырех лет в мире [4], однако, это скорее связано с увеличением числа атак внешнего нарушителя, поскольку невозможно добиться сокращения инцидентов халатного или злоумышленного отношения к конфиденциальным данным одним лишь внедрением технических средств защиты информации [5].

Социальная инженерия. На сегодняшний день на первый план выходит не новый, но редко рассматриваемый источник угроз – социальная инженерия.

Под социальной инженерией здесь и далее будет пониматься инструмент внешнего нарушителя, посредством которого реализуется атака на системы с использованием человеческого фактора, направленный на нарушение конфиденциальности, целостности и (или) доступности информационных ресурсов.

Любую атаку социального инженера условно можно разделить на ряд этапов, представленных на рисунке 2.

Однако, несмотря на одинаковую систему реализации атаки, способы, применяемые в социальной инженерии во многом различаются, среди них особое место занимает Фишинг.

Целевой фишинг – техника в социальной инженерии, направленная на получение сведений конфиденциального характера с применением средств электронной коммуникации, и выступая от другого физического или юридического лица [6].

Основным различием целевого и массового фишинга является то, что при целевом жертвами становятся сотрудники какой-то конкретной, заранее выбранной организации, либо заранее намеченное физическое лицо, в то же время при массовом фишинге жертвами становятся случайные пользователи средств электронной коммуникации [7].

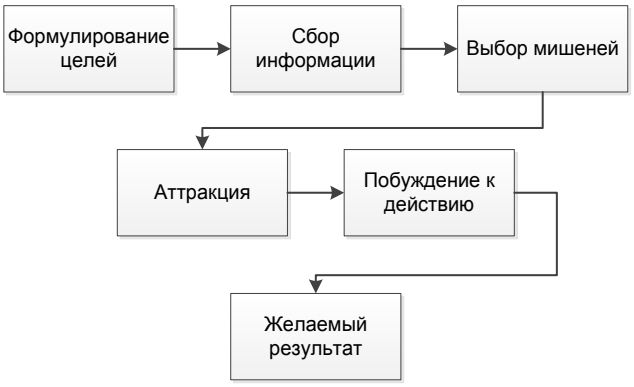


Рис. 3 Основная схема воздействия в социальной инженерии.

Чаще всего фишинг реализовывается посредством электронной почты, непосредственно само письмо содержит в себе вредоносное вложение либо ссылку на фальшивый web-ресурс, содержащий форму с требованием ввести конфиденциальную информацию. Распознать фишинговую атаку бывает проблематично по причине постоянного совершенствования техник. Тем не менее для большинства фишинговых писем характерен ряд признаков:

– сообщение имеет экстренный характер. Это позволяет воздействовать на эмоции пользователя, имитируя стрессовую ситуацию;

– сообщение содержит запрос личных сведений. Это один из самых надежных признаков фишингового письма, так как во многих компаниях запрещено передавать информацию конфиденциального характера по незащищенным каналам связи, и персональные данные в том числе;

– сообщение содержит поддельные URL-адреса, отличающийся от оригинального одним или несколькими символами;

– сообщение содержит изображение в теле письма. Изображение представляет собой гиперссылку на запрещенный ресурс, это необходимо для обхода фильтров «антиспама»;

– сообщение содержит нереалистичные обещания. Примером могут выступать Нигерийские письма, получившие свое название в честь страны, в которой впервые получили массовое распространение и являются примером массового фишинга [8].

– сообщение содержит вложение, в роли которого может выступать вредоносное программное обеспечение. Примечательно то, что расширение вложения может быть скрыто или искусственно изменено, а иконка соответствовать любому неисполняемому файлу, расширение которого указано. Кроме этого, к файлу может быть присоединен ярлык, содержащий настоящее расширение файла. Также вложение может использовать технологию RTLO или RLO (Right-to-Left) для зеркального отображения символов в названии файла. Существует множество других способов изменить вложенный файл, выше перечислена лишь часть из них.

Также фишеры часто использовали эксплоиты, которые могут предоставить доступ уязвимым к процессам и приложениям, а также ко всей операционной системе. Данные угрозы актуальны практически для всех операционных систем, включая Windows, Linux, IOS, MacOS, Android. Многие современные антивирусы снабжены системой защиты от экслоитов, однако пользователи зачатую сами пренебрегают предупреждениями со стороны антивирусных программ. Если они не будут раскрыты, у злоумышленника будет доступ к необходимым ему ресурсам неограниченное время.

По данным на 2013 год в 94% фишинговые письма содержат вредоносные вложения, и только в 6% случаев содержат вредоносные ссылки [9].

Условно к разновидности фишинга можно отнести атаки вида спуфинг.

Спуфинг – вид атаки, реализованной путем подмены адреса отправителя, либо передаваемых пакетов с целью обмана системы безопасности. В зависимости от целей, спуфинг может быть локальным и сетевым. При локальном атака направлена на операционную систему, сетевой спуфиг же направлен на информационную систему в целом.

Одним из основных видов спуфинга являются атаки на транспортный уровень, в частности на протоколы TCP/IP, UDP:

1. NetBIOS/NBNS spoofing – метод, актуальный для ОС Windows, реализовывается во время резолвинга сетевого именипутем подмены DNScервера на ложный. Если запрос к серверу оказался безуспешным, то операционная система попытается реализовать резолвинг с помощью NetBIOS. А злоумышленнику достаточно выдать себя за SOMEPC, во время широковещательного запроса.

2. IP spoofing – атака, реализующаяся с помощью подмены IP-адреса отправителя с целью вызова ответных пакетов на ложный адрес [10]. На этом методе спуфинга построен ряд DoS-атак. Необходимо отметить, что наиболее подвержен атакам этого уровня протокол UDP, так как не имеет механизмов противодействия им. Для защиты от спуфинга IP – адреса является отправка ответного

пакета на адрес отправителя, обычно злоумышленником используется недействительный (случайный) адрес, вследствие чего ответ не придет [11].

3. ARP спуфинг – вид атак в Ethernet сетях, направленный на перехват трафика между отдельными хостами, расположенными в пределах одного широковещательного домена. Базируется на уязвимостях протокола ARP и реализовывается путем подмены mac-адреса. Современные фаерволы способны распознавать данный вид атак. А также минимизировать возможность реализации данной угрозы способно использование arp-таблиц на ключевых частях сети.

4. DNSCachePoisoning (DNS-спуфинг) – атаки, направленные на изменение данных кэша доменных имен. Данный вид атак может быть предотвращен на стороне сервера путем уменьшения степени доверия сторонним данным, а также путем игнорирования любых DNS-записей, не относящихся изначальному запросу [12].

Кроме этого, к фишинговым категориям спуфинга относится подмена e-mailадреса отправителя на ложный. Чаще всего применяется в массовом фишинге, и на сегодняшний день большинство почтовых сервисов оборудовано средствами «антиспама», что позволило минимизировать угрозу со стороны данной категории атак [13].

Также известны случаи спуфинга номеров в VoIP-сетях [14], номеров в SMS-сообщениях и подмены номеров в голосовой почте [15].

Многие направления спуфинга является полноценной самостоятельной атакой, например, GPS спуфинг – атака, направленная на GPS-приемники и реализуется путем использование более мощного передатчика, [16] и Referrer spoofing — подмена реферера [17].

Вишигн – метод фишинговых атак через телефонные коммуникации. Злоумышленник совершает телефонный звонок жертве под видом другого физического, юридического или должностного лица, с которым у жертвы установлены доверительные отношения. Самым надежным способом защиты является не сообщать информацию ограниченного доступа во время телефонных разговоров [18].

Таким образом, получение информации от пользователей возможно не только путем сложных технологических манипуляций, но путем использования банальной невнимательности или халатности субъектов. Что побуждает руководителей и сотрудников службы все большее внимание уделять человеческому фактору, ведь методы социальной инженерии работают везде, где хоть на одном этапе обработки информации присутствует человек.

СПИСОК ЛИТЕРАТУРЫ

1. Громыко И. А. Общая парадигма защиты информации: проблемы защиты информации в аспектах математического моделирования: монография / И. А. Громыко. — Х.: ХНУ имени В. Н. Каразина. 2014. — 216с.
2. Гридин А. Краткое введение в социальную инженерию, 2010. URL: https://habrahabr.ru/post/83415/ (дата обращения 15.09.2017).
3. Глобальное исследование утечек конфиденциальной информации в 2016 году // Аналитический центр InfoWatch, 2017. URL: https://www.infowatch.ru/report2016 (дата обращения 16.09.2017).
4. Утечки данных организаций в результате умышленных или неосторожных действий внутреннего нарушителя. Сравнительное исследование 2013-2015 гг. // Аналитический центр InfoWatch, 2017. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_052016.pdf?rel=1 (дата обращения 16.09.2017).
5. Глобальное исследование утечек конфиденциальной информации в 2014 году // Аналитический центр InfoWatch, 2017. URL: http://ibsmol.ru/InfoWatch_global_report_2014.pdf (дата обращения 16.09.2017).
6. Кузнецов, М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. — Санкт-Петербург: БХВ-Петербург, 2007. — 368 с.
7. Интернет-мошенничество фишинг: механизм, виды и способы противодействия - 2015. URL: https://www.exocur.ru/internet-moshennichestvo-fishing-mehanizm-vidyi-i-sposobyi-protivodeystviya/ (дата обращения 15.09.2017).
8. Кондураке В. П. Защита от фишинг-атак, 2009. URL: http://www.securrity.ru/articles/20-zashhita-ot-fishing-atak.html (дата обращения 17.09.2017).
9. Димов И. Фишинговые методы: сходства, различия и тенденции. Часть вторая: целевой фишинг – 2013 // URL: http://www.securitylab.ru/analytics/440663.php (дата обращения 14.09.2017).
10. Морозов А. В., Шахов В. Г. Анализ атак на беспроводные компьютерные интерфейсы // ОНВ. 2012. №3 (113). URL: http://cyberleninka.ru/article/n/analiz-atak-na-besprovodnye-kompyuternye-interfeysy (дата обращения: 17.09.2017).
11. Хохлов Н. С. Обзор уязвимостей Wi-Fi сигнализации в системах автоматизированного управления зданиями / Хохлов Николай Степанович, Михайлов Дмитрий Михайлович, Смирнов Александр Сергеевич // Вестник ВИ МВД России. 2014. №1. С.277-281.
12. Сапожников А. А. Наблюдение аномалий в сети // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. 2009. №26 (159). С.62-65.
13. Облачный хостинг в Европе (vps/vds) Предотвращение спуфинга адресов и защита электронной почты при помощи SPF-записи. 2016. URL: https://www.8host.com/blog/predotvrashhenie-spufinga-adresov-i-zashhita-elektronnoj-pochty-pri-pomoshhi-spf-zapisi/ (дата обращения: 17.09.2017).
14. Johnny Gabel Hack a Voice-mail Account Using SpoofApp. 2012. URL: https://computer-pranks.wonderhowto.com/how-to/hack-voice-mail-account-using-spoofapp-0133304/ (дата обращения: 17.09.2017).
15. Абдеева З. Р. Проблемы безопасности электронной коммерции в сети Интернет // ПСЭ. 2012. №1. С.172-175.
16. GPS: глушилки, спуфинг и уязвимости // Блог компании Хакспейс Neuron. 2015. URL: https://habrahabr.ru/company/neuronspace/blog/254877/ (дата обращения: 17.09.2017).
17. Christopher Hadnagy Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails / Christopher Hadnagy, Michele Fincher – United States of America, Indiana, Indianapolis: John Wiley & Sons, Inc., 2015. 277 с.
18. Антонов И. О. Способы мошенничества с использованием платёжных карт как элемент криминалистической характеристики данного вида преступлений / Антонов Игорь Олегович, Шалимов Анатолий Николаевич // Учен. зап. Казан. ун-та. Сер. Гуманит. науки. 2013. №4. С.196-203.

УДК 004.056.53

ИСПОЛЬЗОВАНИЕ МОДЕЛЕЙ ВИЗУАЛИЗАЦИИ ДАННЫХ В DLP-СИСТЕМАХ

Коломеец Максим Вадимович
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mail: kolomeec@comsec.spb.ru

Аннотация. В работе рассматриваются примеры визуальной аналитики в DLP-системах. На частных примерах демонстрируется потенциал визуального анализа, и то как использование моделей визуализации позволяет увеличить скорость и улучшить качество принимаемым аналитиком решений. В работе рассматриваются два примера визуальной аналитики в DLP-системах: визуальный анализ времени работы сотрудника с определенными программами и анализ социальных связей на основе рабочего времени сотрудника.

Ключевые слова: *визуальная аналитика; информационная безопасность; предотвращение утечек; DLP; визуализация данных; модели визуализации.*

DATA VISUALIZATION MODELS USAGE IN DLP SYSTEMS

Kolomeec Maxim
ITMO University, Russia, St. Petersburg
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya, 39
e-mail: kolomeec@comsec.spb.ru

Abstract. The paper offers examples of visual analytics for DLP-systems. On specific examples, the potential of visual analysis is demonstrated, and how the use of visualization models allows to increase the speed and improve the quality of decisions made by the analyst. The paper considers two examples of visual analytics in DLP-systems: visual analysis of the employee's time with certain programs and analysis of social connections based on the employee's working time.

Keywords: *visual analytics; information security; prevention of leaks; DLP; visualization of data; visualization models.*

Системы обнаружения и предотвращения утечек информации (Data Leak Prevention - DLP) используют множество методов для повышения эффективности управления предприятием и обеспечения его информационной безопасности. Как правило, DLP-системы выполняют следующие задачи: выявление внутренних злоумышленников, контроль рабочего времени, мониторинг настроений и лояльности сотрудников, резервирование действий сотрудников на случай расследования или несчастного случая. Для выполнения данных задач собираются и анализируются данные сотрудников от множества источников: использование принтеров и съемных носителей, мессенджеры, соцсети, скриншоты и видеозаписи экранов, телефонные звонки, электронная почта, облачные хранилища, файлы персональных компьютеров, данные браузера, сетевого взаимодействия и многие другие.

Такой большой объем данных как правило анализируется специалистами по безопасности при помощи систем автоматического реагирования на несанкционированный доступ к документам или атипичное поведение, а также при помощи правил, реагирующих на смысловое содержание сообщений (посредством поиска ключевых слов, регулярных выражений и схожих инструментов). В данной работе предлагается использование моделей визуализации, которые показывают эффективность визуальной аналитики при анализе поведения сотрудников в рамках DLP-системы.

Визуализация поведения сотрудников. В DLP-системах есть множество способов анализа поведений сотрудников. Это анализ отношений между сотрудниками, анализ атипичного поведения, восстановление последовательности действий и другие.

Рассмотрим частный случай контроля рабочего времени на основе данных об использовании приложений. На персональные компьютеры сотрудников устанавливается агент, который фиксирует запуск приложений.

Таким образом можно косвенно выявить подозрительных сотрудников, путем изменения их шаблона поведения. Как правило, используемые программы выводятся в виде таблицы или круговой диаграммы, отображающей также количество времени, проведенное за той или иной программой (пример круговой диаграммы интерфейса DLP SearchInform [1] использования сотрудником программ изображен на рисунке 1). Для анализа данных за временной промежуток можно использовать потоковые графики, в которых данные выражаются в количественном, а не относительном значении, а также представляют собой временной ряд.

На рисунке 2 изображен потоковый график, на котором шаблон поведения сотрудника прерывается атипичным использованием одной их программ, что может быть основанием для более пристального анализа.

Рисунок 1 – использование сотрудником программ на круговой диаграмме

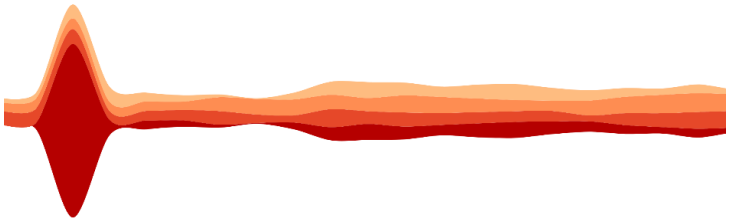


Рисунок 2 – использование сотрудником программ на протяжении недели на потоковом графике

Другой пример – визуализация возможных отношений сотрудников (социальных связей) на основе данных о времени работы и их местоположении. Как правило социальные связи строятся на основе данных об общении посредством мессенджеров, почты и т.п.

Однако немаловажным является анализ на основе данных о местоположении сотрудника (IndoorLocation [2]), поскольку это позволяет определить с кем сотрудник общается вживую. Определить местоположение довольно точно можно с использованием различных технологий: маячкиAppleiBeaconили GoogleEstimote, анализ данных видеонаблюдения при помощиMicrosoftCognitive Services, данные об использовании RFID или NFCкарт для открытия дверей. Количество компаний,которые могут позволить себе такие технологии мало, но с меньшей точностью социальные связи можно определять и на основе времени работы, отмечая вошедших и вышедших сотрудников только на входе. На основе этих данных можно составить интервальный график.

Пример такого графика изображен на рисунке 3. По пересечениям такого графика по оси Y можно сделать выводы о том, как часто могут видеться те или иные сотрудники. На основе пересечений можно составить уже интервальный граф, вершинами которого являются сотрудники, ребра – возможность их встречи, а толщина ребра – времякоторые сотрудники имеют возможность видеться. Интервальный граф, соответствующий интервальному графику на рисунке 3 изображен на рисунке 4.

Рисунок 3 – интервальный график рабочего времени сотрудников

Рисунок 4 – интервальный граф рабочего времени сотрудников

Заключение. В работе рассмотрены модели визуализации, которые могут применяться в DLP-системах для анализа поведения сотрудников и социальных связей между ними. В частности, приведен пример анализа использования сотрудником программ и анализ социальных связей на основе рабочего времени. Таким образом, продемонстрировано что использование визуальной аналитики в DLP-системах имеет потенциал и позволит сократить время и повысить качество анализа. Работа выполнена при финансовой поддержке РНФ (проект 15-11-30029).

СПИСОК ЛИТЕРАТУРЫ

1. Компания «СёрчИнформ».URL: https://searchinform.ru.
2. Муренин И. Н., Новикова Е. С. Визуализация аномальной активности в перемещениях сотрудников критической инфраструктуры //Известия СПбГЭТУ" ЛЭТИ". – 2017. – №. 4. – С. 25-31.

УДК 004.492.3

ПОИСК АНОМАЛИЙ В ПОВЕДЕНИИ ПРОГРАММНОГО ПРОЦЕССА С ПОМОЩЬЮ МАШИННОГО ОБУЧЕНИЯ

Лабутина Евгения Алексеевна
Университет ИТМО
Россия, Санкт-Петербург,Кронверкский пр., 49
e-mail: jenialab@gmail.com

Аннотация. В работе описан алгоритм идентификации процессов программ на основе трасс системных вызовов их потоковдля выявления аномалий в поведении процессов с использованием машинного обучения. Для идентификации использовались модели процессов, простроенные на основе словаря, составленного с помощью алгоритма словарного сжатия Лемпеля-Зива-Уэлча, для распознавания образов нейронная сети типа персептрон.

Ключевые слова: *информационная безопасность; распознавание образов; аномальное поведение; обнаружение аномалий; нейронные сети.*

DETECTION OF ANOMALIES IN BEGAVIOR OF PROGRAM PROCESS USING MASHINE LEARNING

Labutina Eugenia
St. Petersburg State University of Information Technologies, Mechanics and Optics ITMO
Russia, St. Petersburg, Kronverksky pr., 49
e-mail: jenialab@gmail.com

Abstract. The paper describes an algorithm for identifying program processes based on the traces of system calls to their flows to identify anomalies in the behavior of processes using machine learning. For identification, process modelsbased on a dictionary compiled using the Lempel-Ziva-Welch dictionary algorithm were used, for pattern recognition a neural network of the perceptron type.

Keywords: *information security; pattern recognition; anomaly behavior; anomaly detection; neural networks.*

За последние годы возрастает число преступлений в финансовой сфере с нарушением конституционных прав и свобод человека и гражданина, особенно в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий [1]. По данным лаборатории Касперского, 32% пользователей хоть раз за год подвергались вирусной атаке [2]. Современные антивирусы используют сигнатурные алгоритмы обнаружения, при которых происходит поиск уже известных угроз. Поэтому они не способны противостоять целевым атакам и защитить от уязвимостей, которые им еще не известны - 0day уязвимости. Однако даже уязвимости 1-го дня, которые уже были опубликованы и закрыты производителем ПО, представляют опасность из-за того, что администраторы не успевают своевременно обновлять ПО. Поэтому очень важно вовремя обнаружить вирус. Одним из наиболее перспективных направлений в области обнаружения вредоносных программ является поиск аномалий в работе процессов ОС.

В ходе работы был предложен детектор, который подстраивается под защищаемую систему и способен находить аномалии в поведении процессов операционной системы. Сбор данных о поведении процессов системы происходил с помощью программы для записи системных вызовов, описанной в работе [3]. Назовем множество системных вызовов ОС за ограниченный период времени снимком системы. Для составления признаков по снимку был применен алгоритм словарного сжатия LZW (Лемпеля-Зива-Уэлча), описанный в работе [4]. Была составлена модель системы – это множество словарей для некоторого обучающего снимка. Распознавание процессов по этой модели проводилось на основе следующих признаков: количество новых символов вторичного словаря, средняя длина символов вторичного словаря, максимальная длина новых символов вторичного словаря, длина трассы потока тестового снимка. Признаки были выписаны в кортежи, подавались на вход нейронной сети типа персептрон. Она была обучена методом обратного распространения ошибки. На выходе ожидалась 1, если кортеж устанавливает принадлежность трасы модели системы, и 0 в противном случае. (Если pidи tidсовпадают.) Для проверки качества обучения выберем 20% векторов. Был выбран некоторый порог THR, если выход нейронной сети для некоторого вектора был больше THR, то считаем гипотезу о принадлежности трасы модели системы верной. Переборным алгоритмом была выбрана лучшая нейросеть. Её точность распознавания составила 0.82.

Также были записаны трассы вредоносной программы Trojan.Winlocker.При распознавании ее трасс нейронная сеть выдала значение не более 0.021 на выходе, что говорит о том, что среди ранее изученных процессов нет и отдаленно похожего на вредоносный. Был проведен тест, показывающий, насколько процесс, который не участвовал в составлении обучающего снимка, распознается моделью. Была записана работа программы Firefoxв течение минуты. Был оценен каждый поток получившегося процесса в моделях всех потоков обучающего снимка. На графике 10 отмечены точки,

показывающие зависимость выхода нейронной сети от длины потока программы Firefox. В отличие от вредоносной программы, для которой выход нейронной сети в каждом из случаев был порядка 0.02, некоторые потоки данной программы распознаются моделью с достаточно высокой точностью.

Рис.1. Оценка всех потоков Firefoxво всех моделях обучающего снимка

В итоге был разработан алгоритм построения моделей процессов на основетрасс их потоков по алгоритму LZW.

Точность в 0.82 не соответствует требованиям к точности более 0.99, требуемой для промышленного применения алгоритма. Однако составление обучающей выборки при обучении с учителем производилось недостаточно точно, поскольку нам заранее не известно, должны ли 2 потока с разными pid и tid друг другу соответствовать. Так, например, в работе [3] обучающая выборка составлялась по именам процессов, что дало более высокую точность.

Разработка данного метода имеет важный прикладной потенциал. Достижение точности более 0.99 позволит обнаружить вредоносные программы без сигнатур только на основе машинного обучения. При этом со временем качество распознавания будет увеличиваться.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности РФ. Утв. Указом Президента РФ от 05.12.2016 № 646. Режим доступа [Электронный ресурс] / URL: http://www.kremlin.ru/acts/bank/41460/page/2, режим доступа: свободный, дата обращения: 10.05.17.
2. Kasperskysecuritybulletin 2016. Статистика. [Электронный ресурс] / URL: https://go.kaspersky.com/RU_Security_Bulletin_2016_Stats_SOC_2016.html, режим доступа: свободный, дата обращения: 24.06.17
3. Баклановский М.В., Ханов А.Р., Комаров К.М., Лозов П.А. Оценка точности алгоритма распознавания вредоносных программ на основе поиска аномалий в работе процессов // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 5. С. 823–830. doi: 10.17586/2226-1494-2016-16-5-823-830
4. Мастрюков Д. Алгоритм LZW. Краткое описание алгоритма LZW и его реализации. Алгоритмы сжатия информации. Часть 4. Алгоритм LZW//Монитор, N3, 1994. С8-11.

УДК 004.056.53

ПОДХОД К ПРОЕКТИРОВАНИЮ ЗАЩИЩЕННЫХ СИСТЕМ НА ОСНОВЕ ВСТРОЕННЫХ УСТРОЙСТВ

Левшун Дмитрий Сергеевич
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14 линия, 39
e-mail: levshun@comsec.spb.ru

Аннотация. В данной работепроанализированы современные подходы к проектированию защищенных встроенных устройств, а также к разработке безопасного программного обеспечения с точки зрения их применимости к задаче проектирования защищенных систем на основе встроенных устройств. Проанализированы существующие подходы к проектированию защищенных систем на основе встроенных устройств. Предложен новый подход к проектированию защищенных систем на основе встроенных устройств.

Ключевые слова: *киберфизические системы; встроенные устройства; проектирование защищенных систем; безопасность систем на основе встроенных устройств.*

THE APPROACH TO DESIGN OFSECURE SYSTEMSBASED ON EMBEDDED DEVICES

Levshun Dmitry
St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia,St.-Petersburg, Kronverkskiy, 49
St. Petersburg Institute for Informatics and Automation of Russian Academy of Science,
Russia,St.-Petersburg, 14th Liniya,39
e-mail: levshun@comsec.spb.ru

Abstract. The article is devoted to analysis of approaches to design of the secure embedded devices, as well as the development secure software in terms of applicability to the problem of designing secure systems based on embedded devices. The existing approaches to the design of secure systems based on embedded devices are analyzed. The new approach to the design of secure systems based on embedded devices is proposed.

Keywords: *cyberphysical systems; embedded devices; development of secure systems; security of systems based on embedded devices.*

В настоящее время широкое распространение получил комплексный подход к обеспечению киберфизической безопасности критически важных инфраструктур.

Данный подход заключается в объединении в рамках единой системы гетерогенных источников событий физического и кибернетического уровня, а также в обеспечении устойчивости таких систем к атакам на них [1].

Применение данного подхода позволяет выявлять инциденты безопасности, сценарии атак, а также аномальную активность, обнаружение которых ранее было возможно только на этапах расследования, и реагировать на них в режиме реального времени [2].

При этом для разработки безопасного программного обеспечения существуют государственные и международные стандарты, а также решения от ведущих компаний в области информационных технологий. Кроме того, широкое распространение получили фреймворки для проектирования архитектуры программного обеспечения с учетом необходимости обеспечения его безопасности.

К сожалению, функциональность встроенных устройств определяется не только программной, но и аппаратной составляющей.

При этом связи между программной частью устройства, с одной стороны, и аппаратной, с другой, обуславливают наличие дополнительных ограничений, влияющих существенным образом на процесс проектирования таких устройств.

Это означает, что существующие решения для разработки безопасного программного обеспечения не применимы для разработки безопасных систем на основе встроенных устройств в полной мере, а потому нуждаются в доработке.

Также на практике применяется методики, которые позволяют ещё на этапе проектирования встроенного устройства выявлять перечень возможных атак, которым может быть подвержено устройство, в соответствии с выбранной моделью нарушителя, а также используемыми программно-аппаратными компонентами [3]. Однако применение подобных методик и дальнейшее объединение в рамках единой системы множества защищенных встроенных устройств не позволяет разработать защищенную систему из-за необходимости учета эмерджентных свойств полученной системы. А это означает, что данные методики также не применимы к поставленной задаче в полной мере и нуждаются в доработке.

Кроме того, в последнее время широкое распространение получили исследования в области методик разработки и верификации сетевых систем на основе встроенных устройств [4].

Основной целью данных методик является предоставление разработчикам сетевых систем на основе встроенных устройств информации о применимости отдельных интерфейсов и протоколов передачи данных для обеспечения соответствующего уровня надежности итоговой системы. При этом безопасность системы встроенных устройств не является непосредственной целью данных методик, однако отдельные аспекты безопасности учитываются при выборе интерфейсов и протоколов передачи данных.

Также важно отметить, что методики данного типа позволяют обеспечить надежность только изолированных систем встроенных устройств, не рассматривая их взаимодействие с удаленными серверами, рабочими станциями, веб-сервисами и т.п.

Это означает, что методики разработки и верификации сетевых систем на основе встроенных устройств не применимы для задачи обеспечения защищенности не изолированных систем на основе встроенных устройств, а потому также нуждаются в доработке.

На рис. 1 представлен разработанный подход к проектированию защищенных систем на основе встроенных устройств:

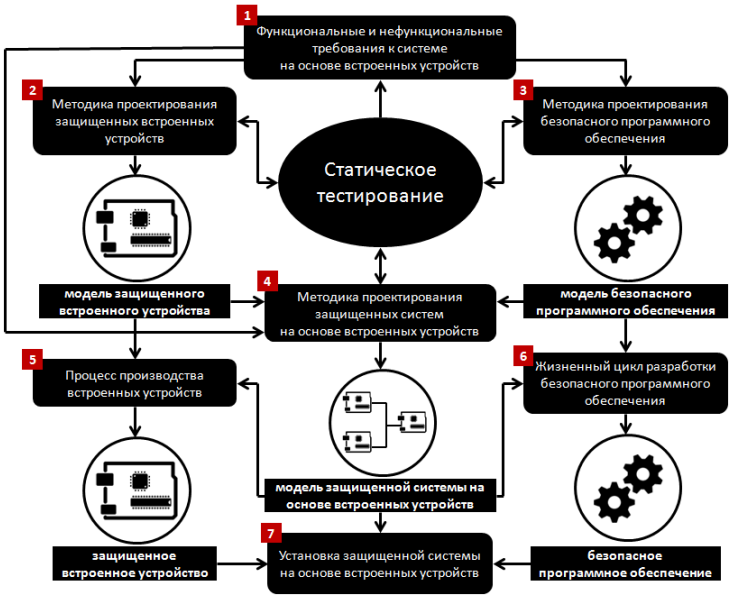


Рис. 1. Подход к проектированию защищенных систем на основе встроенных устройств

Подытоживая вышесказанное, важно отметить, что на данный момент не существует единого обобщенного подхода для решения задачи проектирования защищенных систем на основе встроенных устройств, а существующие частные решения не лишены недостатков и нуждаются в доработке. В данной работепредложен обобщенный подход к проектированию защищенных систем на основе встроенных устройств. Новизной предложенного подхода является объединение решений по разработке безопасного программного обеспечения с методиками проектирования защищенных встроенных устройств в единую методику проектирования.При этом в качестве эмерджентных свойств рассматриваются свойства, проявляющиеся в системе на основе интерфейсов и каналов передачи данных между элементами системы.

Работа выполнена при поддержке гранта РНФ №15-11-30029 в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Vasily Desnitsky, Dmitry Levshun, Andrey Chechulin and Igor Kotenko. Design Technique for Secure Embedded Devices: Application for Creation of Integrated Cyber-Physical Security System. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol.7, No.2, June, 2016. P.60-80. http://jowua.yolasite.com/vol7no2.php
2. Igor Kotenko, Dmitry Levshun, Andrey Chechulin. Event correlation in the integrated cyber-physical security system. Proceedings of the 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM-2016), IEEE, St. Petersburg, Russia, May 2016. P.484-486.
3. Vasily Desnitsky, Andrey Chechulin, Igor Kotenko, Dmitry Levshun, Maxim Kolomeec. Application of a Technique for Secure Embedded Device Design Based on Combining Security Components for Creation of a Perimeter Protection System. 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP 2016). Heraklion, Crete, Greece, February, 2016. IEEE Computer Society. 2016. P. 609-616.
4. Francesco Stefanni. A Design & Verification Methology for Networked Embedded Systems. Ph.D. Thesis. University of Verona, Department of Computer Science, Italy. April 7, 2011. PP. 143.

УДК 004.75

ОРГАНИЗАЦИЯ КОЛЛЕКТИВНОГО УПРАВЛЕНИЯ БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ

Мариненков Егор Денисович, Шуваев Александр Константинович
Университет ИТМО
Россия, Санкт-Петербург, ул. Ломоносова, 9
e-mails: egormarinenkov@niuitmo.ru, arcshev@niuitmo.ru

Аннотация. В работе рассмотрен алгоритм организации движения беспилотных летательных аппаратов на основе децентрализованного метода управления, использование которого позволяет отказаться от использования центрального управляющего устройства. Отказ от центрального управляющего устройства позволяет говорить об отсутствии критического элемента, что повышает устойчивость системы к реализации угроз информационной безопасности. Разработанный алгоритм был реализован в системе управления группой БПЛА.

Ключевые слова: *беспилотные летательные аппараты; мультиагентный подход; самоорганизующиеся системы.*

ORGANIZATION OF COLLECTIVE MANAGEMENTBASED ON UNMANNED AERIAL VEHICLES

Marinenkov Egor, Shuvaev Alexander
ITMO university
Russia, St. Petersburg, Lomonosova str., 9
e-mails: egormarinenkov@niuitmo.ru, arcshev@niuitmo.ru

Abstract. The article proposed algorithm of unmanned aerial vehicles motion control based on decentralized control method, which allow to refuse the usage of central control unit. The refusing from the central control unit means absence of critical element that improves the stability of the system in case of information security threats realization. Authors implement developed algorithm in the control system of drones group.

Keywords: *unmanned aerial vehicles; multi-agent approach; self-organized system.*

Авторы работы рассматривают применение беспилотных летательных аппаратов (БПЛА) как самоорганизующейся группы, способной решать задачи, нехарактерные для любого участника данной группы, в частности. Данная тематика стала развитием парадигмы применения мобильных робототехнических систем в пространстве, а не в плоскости.

Одной из главных задач управления коллективом БПЛА является бесконфликтное движение в пространстве [1]. Таким образом, формулируется цель исследования – разработка алгоритма беспрепятственного движения группы БПЛА в пространстве с учетом дополнительных ограничений, накладываемых на возможное расположение аппаратов. Для достижения поставленной цели были сформулированы следующие задачи:

– определение подхода к организации коллективного управления БПЛА;

– разработка алгоритма предотвращения столкновений с другими элементами, находящимисяв воздушном пространстве;

– определение информации, необходимой для функционирования разрабатываемого алгоритма;

– реализация предложенного алгоритма.

Достижение цели исследования предполагает разработку подхода к разлету БПЛА на основе самоорганизующейся коллаборации. В работе [2] рассматривается один из возможных подходов к организации дорожного движения на основе беспилотных транспортных средств (БТС). Данный подход позволяет обеспечивать бесконфликтное движение БТС на плоскости, но он не адаптирован для использования в трехмерном пространстве. Для формирования подхода к организации бесконфликтного движения БПЛА необходимо рассмотреть общие принципы построения информационного взаимодействия (ИВ) аппаратов, и определить возможные критерии, согласно которым будут определяться оптимальные маршруты следования, сформулировать показатели эффективности.

Постановка задачи организации движения в трехмерном пространстве. Перед постановкой задачи авторы рассматривают методы группового управления, описанные в работе [3], с целью выявить удовлетворяющую стратегию для достижения поставленной цели. Проанализировав возможные подходы к организации группового управления, авторы рассматривают децентрализованную коллективную стратегию в качестве основы для построения алгоритма движения группы БПЛА, в связи с ее преимуществами:

– время принятия решения линейно зависит от количества объектов в группе;

– в связи с отсутствием центрального управляющего устройства повышается отказоустойчивость системы;

– наличие общего канала информации позволяет реализовать взаимодействие между объектами коллаборации, что позволяет говорить о возможности выработки оптимальных маршрутов движения БПЛА.

В работе авторы формулируют систему ограничений и допущений для задачи управления движением в трехмерном пространстве на основе БПЛА.

Рассматривается система «БПЛА – перекресток коридоров» и процессы в ней как дискретные, т.е. ограничиваясь их значениями в фиксированные моменты времени t_k, t_k+1, t_k+2, … . В каждый момент времени t_k+f, каждый беспилотник может занимать один или несколько элементарных блоков пространства (ЭБП). Каждый ЭБП имеет номер вида *ijk*, где,*i* – координата ЭБП по оси *X*, *j* – координата ЭБП по оси *y*, *k* – координата ЭБП по оси *Z*. Скорости перемещения каждого беспилотника при движении равны друг другу и равны *const* (при *const≠0*).

Формулируя правила направления полета БПЛА в воздушном пространстве, авторы вводят следующие ограничения:

– при перемещении без изменения высоты, т.е. в плоскости O_{xy}, вводится правило правостороннего движения;

– при изменении высоты, рассматривается плоскость O_{xz}и вводится правило левостороннего движения, которое распространяется только на ось O_z;

– не подразумевается движение по диагонали, следовательно, № ЭБП в момент времени t_k+1 будет иметь вид *i+1jk*, или *ij+1k*, или *ijk+1*, или *ijk* (если БПЛА зависает), при условии, что в момент времени t_kномер ЭБП равен *ijk*.

Главной задачей организации управления является перевод системы роботизированных БПЛА из некоторого начального состояния в заданное конечное так, чтобы некая целевая функция *Y*достигала наибольшего значения с учетом принятых ограничений.

В соответствии с указанной выше децентрализованной моделью управления, каждый приближающийся к перекрестку БПЛА после процедуры идентификации обменивается информацией о своем текущем состоянии S_iи выбранных в данный момент времени действиях A_i.

Данную информацию, беспилотник передает остальным участникам движения в виде протокола, где находятся такие параметры, как *id*, *cur_pos*, *tar_pos*, *t*.

В данном протоколе *id* – идентификационный номер БПЛА, *cur_pos* – № ЭБП, в котором находится БПЛА, *tar_pos* - № ЭБП, в котором БПЛА окажется после прохождения перекрестка, *t* – время прибытия БПЛА на перекресток. После обмена сообщениями в ячейках памяти каждого БПЛА содержится информация о всех БПЛА группы.

При наличии *N*квадрокоптеров в группе, намеревающихся преодолеть перекресток, в какие-то моменты времени возможна ситуация, когда несколько квадрокоптеров могут претендовать на один и тот же ЭБП. Для разрешения данного конфликта необходимо указать приоритет пролета перекрестка. Для выбора наиболее эффективного приоритета строится дерево всех возможных вариантов маршрутов, где вершина – конфликт, который необходимо разрешить, узлы – возможные приоритеты, листья – приоритеты, ведущие к бесконфликтному пересечению перекрестка всеми БПЛА. После построения дерева имеется набор вариантов приоритета, удовлетворяющих разрешению конфликта. Чтобы выявить наиболее эффективный вариант необходимо рассчитать значения целевой функции *Y*, который означает пропускную способность перекрестка. Значение данного функционала зависит от количества ЭБП, которые были пройдены каждым БПЛА в пространстве с учетом дополнительных ограничений, накладываемых, и количества дискрет времени затраченных на пересечение перекрестка. Совокупность маршрутов, при которой достигается максимальное значение целевой функции, считается наиболее эффективной и принимается к исполнению всеми БПЛА.

Заключение. Авторами был выделен метод группового управления, на основе которого был разработан алгоритм беспрепятственного движения группы БПЛА через трехмерный перекресток воздушных коридоров с учетом дополнительных ограничений, накладываемых на возможное расположение аппаратов. Рассматривая систему децентрализованной коллективной стратегии, была выявлена уязвимость общего канала обмена информацией. Дальнейшие исследования будут направлены на обеспечение информационной безопасности группы БПЛА.

СПИСОК ЛИТЕРАТУРЫ

1. Ватаманюк И. В., Панина Г. Ю., Ронжин А. Л. Реконфигурация пространственного положения роя роботов //Управление большими системами: сборник трудов. – 2015. – №. 58.
2. Зикратов И. А., Викснин И. И., Зикратова Т. В. Мультиагентное планирование проезда перекрестка дорог беспилотными транспортными средствами //Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Т. 16. – №. 5.
3. Каляев И. А., Гайдук А. Р., Капустян С. Г. Модели и алгоритмы коллективного управления в группах роботов. Монография. – 2009.

УДК 004.492.3

ИССЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ СИСТЕМ УПРАВЛЕНИЯ МОБИЛЬНЫМИ УСТРОЙСТВАМИ

Медведев Михаил Сергеевич, Бежан Роман Романович, Арустамов Сергей Аркадьевич
Университет ИТМО
Россия, Санкт-Петербург, Кронверкские пр., 49
e-mails: mmedvedev.793@mail.ru, romanbezhan@gmail.com, sergey.arustamov@gmail.com

Аннотация. Рассмотрены результаты проведенного исследования защищённости систем управления мобильными устройствами от возможных видов атак и существующие меры противодействия им, а также продемонстрированы уязвимости в корпоративных системах. В качестве исследуемых систем были использованы наиболее популярные в мире продукты компании Sap: SapMobilePlatform и SapAfaria. Практическая значимость работы для информационной безопасности заключается в акцентировании внимания на проблему защищенности критичных данных, обрабатываемых ERP системами.

Ключевые слова: *Sap; Sap Mobile Platform; Sap Afaria: мобильные устройства; MDM.*

INVESTIGATION OF PROTECTION OF CONTROL SYSTEMSMOBILE DEVICES

Medvedev Mikhail, Bezhan Roman, Arustamov Sergey
St. Petersburg State University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverkskiy pr.,49
e-mails: mmedvedev.793@mail.ru, romanbezhan@gmail.com, sergey.arustamov@gmail.com

Abstract. The paper examines the results of a study of the security of mobile device management systems against possible types of attacks and the existing measures to counter them, as well as demonstrated vulnerabilities in corporate systems. As the systems under investigation, the most popular products of the company Sap were used: Sap Mobile Platform and Sap Afaria. The practical importance of the work for information security is to focus on the problem of the security of critical data processed by ERP systems.

Keywords: *Sap; Sap Mobile Platform; Sap Afaria: mobile devices; MDM.*

В настоящее время информационные технологии все глубже проникают в нашу жизнь, почти каждый обладает носимым устройством, будь то смартфон, планшет, ноутбук или даже умные часы. Поэтому в современных организациях и предприятиях снабжают своих сотрудников многофункциональными носимыми устройствами, которые позволяют им быть неотрывными от процесса производства и оперативно принимать решения. Для решения проблемы, удаленного контроля и управления носимыми устройствами, существует множество различных предложений, но лидерами, в данной области, являются продукты компании Sap: Sap Mobile Platformи Sap Afaria.

Sap Mobile Platform – обеспечивает передачу информации от баз данных и информационных систем к приложениям на конечных устройствах пользователей, а также организует взаимодействие различными устройствами [1].

Sap Afaria – это MDM решение, которое позволяет обеспечивать контроль и защиту мобильных устройств, используемых сотрудниками организаций [2].

В связи с высокой критичностью данных, проходящих через системы управления мобильными устройствами и привязанных к ним мобильных устройств, безопасность данных систем нельзя оставить без внимания.

В случае получения неправомерного доступа к системам, злоумышленник может нанести непоправимый ущерб, позволив недоброжелателям, либо конкурентам полностью парализовать работу организаций и предприятий.

Для предотвращения различных потерь, при использовании систем управления мобильными устройствами, необходимо было исследовать насколько безопасно осуществляется передача и хранение критичной информации в данных системах и насколько устойчивы они к различным видам атак.

В процессе работы был построен лабораторный стенд, состоящий из виртуального сервера«Windows Server 2008», смартфона «Nexus 5» с операционной системой «Android 6.0 Marshmallow» и эмулятора мобильного телефона с операционной системой «Android 6.0 Marshmallow» развернутого в «Android Studio».

В данной работе были проведены исследования защищённости систем управления мобильными от различных видов атак: со стороны носимого устройства на удалённые сервера; с серверов на удаленные мобильные устройства; атаки с внедрением между серверами и мобильными устройствами и существующие меры противодействия им.

В ходе проведения исследования защищенности систем управления мобильными устройствами автором были найдены уязвимости, позволяющие нанести огромный вред предприятию использующие данную систему для управления мобильными устройствами. Найденные уязвимости были отправлены разработчику для исправления ошибок, влекущих за собой угрозы для организаций, использующих данные системы.

Результат исследования служит для повышения уровня защищенности систем управления мобильными устройствами.

Анализ безопасности Sap Afaria и Sap Mobile Platform, показал, что защита информации должна происходить так же и на уровне приложений, которые обрабатывают эти данные.

СПИСОК ЛИТЕРАТУРЫ

1. SAP, SAP Mobile Platform [Электронный ресурс] — Режим доступа: https://www.sap.com/products/mobile-app-development-platform.html#item_0 (15.09.2017).
2. Afaria Wiki, Afaria Architecture [Электронный ресурс]— Режим доступа: http://afaria.wikia.com/wiki/Afaria_Wiki (15.09.2017).

УДК 004.056

ОЦЕНКА РИСКОВ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ И МЕТОДОЛОГИЙ

Мелешко Алексей Викторович, Чумак Евгений Александрович, Савков Сергей Витальевич
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: lexa.0710@gmail.com, eugenich@ya.ru,sergsavkov@gmail.com

Аннотация. В работе рассмотрены различные подходы к определению понятия «риск» и методы оценки информационных рисков. Изучен математический аппарат методик оценки риска, выявлены преимущества и недостатки каждой методики. На основе проведенного исследования были сделаны выводы о плюсах и минусах рассмотренных методик, а также о том каким образом в них оценивается риск.

Ключевые слова: *безопасность; риск; оценка риска; методики оценивания риска.*

ASSESSMENTOF RISKS: COMPARATIVE ANALYSIS OF APPROACHES AND METHODOLOGIES

Meleshko Aleksei, Chumak Evgeny, Savkov Sergey
St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverksky pr.,49
e-mails: lexa.0710@gmail.com, eugenich@ya.ru, sergsavkov@gmail.com

Abstract. Different approaches to the definition of the concept of "risk" and methods for assessing information risks are considered in the article. The mathematical apparatus of risk assessment methods has been studied, the advantages and disadvantages of each method have been revealed. Based on the study, conclusions were drawn about the pros and cons of the methods examined, as well as how they assess the risk in them.

Keywords: *security; risk; risk assessment.*

В процессе управления крупным предприятием или же простым проектом люди сталкиваются с различными угрозами безопасности. Преднамеренные, непреднамеренные, стихийные угрозы, в случае их возникновения и реализации, могут нанести вред информации, хранящейся и обрабатываемой на предприятии, а также предприятию в целом. Для того, чтобы избежать потерь, необходимо оценить вероятность возникновения той или иной угрозы и правильно построить систему защиты информации на предприятии.

Вероятность возникновения угрозы ассоциируется с понятием риска. Например, в ГОСТ Р ИСО/МЭК 27005-2010 под риском понимается возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации. Поэтому оценка возникновения угроз безопасности сводится к понятию оценки риска информационных систем.

Существует множество подходов и методик оценки информационного риска. На сегодняшний день можно выделить следующие, наиболее распространенные подходы к оценке риска: аксиоматический подход, эмпирический подход, подход на основе Value at Risk (стоимостная мера риска), подход на основе подход на основе ожидаемых потерь. Так же в докладе рассмотрены методики оценки информационных рисков.

В целом методики оценки риска делятся на методы количественной оценки и методы качественной оценки риска. Качественные методы позволяют выявить источники возникновения риска, возможный ущерб, а также выработать меры по снижению риска. Количественные методы позволяют численно оценить влияние факторов риска на систему. Зачастую качественная оценка риска является основой для проведения количественного анализа.

К качественным методам оценки риска можно отнести следующие методы: метод экспертных оценок, метод рейтинговых оценок, контрольные списки источников, и другие. Метод экспертных оценок направлен на получение мнения экспертов по определенному кругу вопросов. Метод рейтинговых оценок можно считать разновидностью метода экспертных оценок.

В данном методе зачастую используют систему оценок в баллах. Результатом является таблица «рейтинг рисков».

Метод «контрольные списки источников» базируется на использования списка рисков, составленных ранее, то есть использует данных исторического характера. Анализируются факторы риска, которые были выявлены ранее и из последствия.

Количественные методы оценки риска можно разделить на статистические методы, аналитические методы. Аналитические методы позволяют определить вероятность возникновения риска на основе математических моделей.

Статистические метода определяют вероятность возникновения риска на основе статистических данных. Данные методы оперируют такими понятиями как среднее математическое ожидание и изменчивость возможного результата.

К конкретным количественным методам оценки риска можно отнести метод имитационного моделирования, метод достоверных эквивалентов, анализ чувствительности, метод корректировки нормы дисконта с учетом риска и другие.

Метод достоверных эквивалентов основан на использовании специальных понижающих коэффициентов (коэффициентов достоверности). В качестве таких коэффициентов чаще всего используют математическое ожидание.

Метод имитационного моделирования основан на построении модели, состоящей из случайных величин, над которыми проводится серия экспериментов с целью выявления влияния исходных данных на зависящие от них величины. Анализ чувствительности дает оценку влияния исходных параметров проекта на его конечные характеристики. То есть данный метод позволяет понять, как меняются показатели эффективности при изменении входных данных.

В докладе рассмотрены подходы и методики оценки риска, которые позволяют оценить влияние того или иного фактора риска на информационную систему, что в свою очередь поможет правильно организовать защиты системы.

Результатом работы рассмотренных методик является либо конечное число (у количественных методов) либо оценка эксперта, например балл (метод экспертных оценок), то есть оценивают риск качественно или количественно.

Однако существует альтернативный подход к оценке риска – стохастический. Его суть заключается в том, что риск рассматривается несколько иначе, как случайная величина и оценка риска осуществляется в виде вероятностного распределения, которое показывает влияние фактора риска на свойства объекта. Используя стохастический подход можно предоставить эксперту свободу выбора способа оценивания влияния факторов риска, тем самым получить больше знаний от эксперта, а, следовательно, более точную оценку.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011 – 51с.
2. Мадера, А.Г. Риски и шансы. Неопределенность, прогнозирование и оценка: Учебное пособие – М.: URSS, 2014 - 448 с.

УДК 004.56

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ WSN-СЕТЕЙ НА ОСНОВЕ МОДЕЛИ ДОВЕРИЯ

Овасапян Тигран Джаникович, Иванов Денис Вадимович, Зегжда Дмитрий Петрович
Санкт-Петербургский политехнический университет Петра Великого
Россия, Санкт-Петербург, ул. Политехническая, 29
e-mails: ovasapyan.t@gmail.com, 9361023@gmail.com, dmitry@ibks.ftk.spbstu.ru

Аннотация. Рассматривается обеспечение безопасности беспроводных сенсорных сетей с использованием модели доверия. Авторами проведен анализ принципов функционирования сенсорных сетей и построена классификация методов маршрутизации. Проанализированы типовые угрозы и выявлены актуальные атаки на WSN-сети. Рассмотрены существующие методы обеспечения безопасности и определены их недостатки. Разработан метод обеспечения защиты от вредоносных узлов с использованием модели доверия. Проведена экспериментальная оценка эффективности разработанного метода, путем моделирования его работы в симуляторе WSN-сети.

Ключевые слова: *беспроводные сенсорные сети; WSN-сети; протоколы маршрутизации ;модель угроз; модель доверия.*

SECURITY FOR WSN BASED ON THE TRUST MODEL

Ovasapyan Tigran, Ivanov Denis,Zegzhda Dmitry
Peter the Great St. Petersburg Polytechnic University
Russia, St. Petersburg, Polytechnicheskaya str., 29
e-mails: ovasapyan.t@gmail.com, 9361023@gmail.com, dmitry@ibks.ftk.spbstu.ru

Abstract. The paper deals with ensuring the cybersecurity of a wireless sensor network using a trust model. The authors analyzed the principles of the functioning of wireless sensor networks, and classified routing methods. Typical threats were analyzed and actual attacks on wireless sensor networks were found out. Existing safety methods were reviewed and their disadvantages were defined. Safety method of malicious nodes protection with usage of trust model was worked out. Experimental estimation of effectiveness of the worked out method was performed on the basis of modeling its operation in the simulated wireless sensor network.

Keywords: *wireless sensor networks; WSN; routing protocols; threat model; trust model.*

Актуальность решения задач, связанных с построением распределенных систем контроля и мониторинга чрезвычайных ситуаций, критических параметров производственных процессов и различных экологических показателей трудно переоценить. Использование традиционных проводных

решений далеко не всегда эффективно из-за неудобства, а также высокой стоимости развертывания и технического обслуживания. Беспроводные сенсорные сети (Wireless Sensor Network, WSN) являются новым классом беспроводных сетей передачи информации, позволяющие объединить большое число относительно простых датчиков в единую сеть.

Наряду с развитием Интернета вещей (Internet of Things, IoT), WSN-сети все активнее внедряются в окружающую среду. WSN-сети как часть Интернета вещей займут важнейшее место в сетях связи уже в среднесрочной перспективе, в связи с широким спектром областей применения данного типа сетей, а также минимальными затратами, необходимыми при развертывании сети и последующем ее сопровождении в процессе эксплуатации.

В связи со спецификой WSN-сетей, использование традиционных средств защиты не способно обеспечить должный уровень безопасности построенной инфраструктуры. Помимо таких угроз как уязвимость прослушивания каналов передачи данных и подмены трафика, характерных для классических беспроводных сетей, WSN-сети могут быть подвержены ряду других угроз, из-за следующих особенностей [1]:

– необходимость использования сложных алгоритмов маршрутизации из-за динамически изменяющейся топологии сети;

– невозможность использования таких систем безопасности, как центры сертификации и центральные серверы, из-за отсутствия необходимой инфраструктуры;

– незащищённость от злоумышленников, способных получить физический доступ к узлам WSN-сети;

– критичность узлов сети по отношению к энергетическим и вычислительным ресурсам.

Проанализированы типовые угрозы в беспроводных сенсорных сетях [2]. Авторами доклада разработана классификация актуальных угроз безопасности WSN-сетей, которая систематизирует данные о возможностях и целях нарушителей, а также определяет возможные способы реализации угроз безопасности. На основе выявленных угроз определены основные атаки, которые направлены на выведение из строя беспроводных узлов сети, дезориентацию протоколов маршрутизации, а также сбой работы сети в целом.

Использование множества различных существующих методов защиты от конкретных атак в WSN-сетях далеко не всегда является целесообразным из-за ограниченности узлов в ресурсах. Некоторые из рассмотренных методов защиты не имеют на сегодняшний день ни одной практической реализации. Другие методы противоречат друг другу, например, по требуемым протоколам маршрутизации, что делает невозможным их одновременную работу в рамках одной сети. К тому же обновление функционала, для противодействия новым атакам, требует физического доступа к некоторым узлам, что не всегда представляется возможным и увеличит стоимость обслуживания сети. В связи с этим необходим универсальный механизм обеспечения безопасности, позволяющий защитить WSN-сети от подавляющего большинства атак.

Проанализированы модели обеспечения безопасности в децентрализованных сетях, такие как модель Ксюдонга [3], товарищеская модель безопасности [4], модель доверия [5]. Наиболее подходящим под концепцию WSN-сетей является механизм, основанный на определении уровня доверия узлов друг к другу с использованием метрик доверия.

Для оценки эффективности метода защиты WSN-сетей на основе модели доверия смоделирована работа WSN-сети в эмуляторе. В качестве инструмента моделирования используется пакет Network Simulator 2 (NS-2). Смоделированная сеть состоит из узлов-сенсоров, базовой станции и узлов злоумышленника. Поведение злоумышленника изменялось путем реализации различных атак, поддерживаемых эмулятором. Результаты моделирования показали, что сеть успешно выявляет вредоносные узлы и 80% пакетов в сети остаются нетронутыми с учетом того, что 25% узлов являются атакующими. Помимо того, что сеть сохраняет работоспособность, количество энергии, потребляемое каждым узлом сети, также показывает адекватные результаты.

СПИСОК ЛИТЕРАТУРЫ

1. Постольский С. П. Обзор проблемных областей в безопасности беспроводных сенсорных сетей, классификация атак, описание атак сетевого уровня. – u-conferences. org/CSPS, 2015.
2. Kocher I. S. et al. Threat models and security issues in wireless sensor networks //International Journal of Computer Theory and Engineering. – 2013. – Т. 5. – №. 5. – С. 830.
3. Guan X., Yang Y., You J. POM-a mobile agent security model against malicious hosts //High Performance Computing in the Asia-Pacific Region, 2000. Proceedings. The Fourth International Conference/Exhibition on. – IEEE, 2000. – Т. 2. – С. 1165-1166.
4. Page J., Zaslavsky A., Indrawan M. A buddy model of security for mobile agent communities operating in pervasive scenarios //Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation-Volume 32. – Australian Computer Society, Inc., 2004. – С. 17-25.
5. Rani V. U., Sundaram K. S. Review of trust models in wireless sensor networks //Int. J. Comput. Inf. Syst. Control Eng. – 2014. – Т. 8. – С. 371-377.

УДК 004.056.53

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Орлов Иван Алексеевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, ул. Большая Морская, 67, лит. А
e-mail: like12341@mail.ru

Аннотация. Статья посвящена применению искусственных нейронных сетей и вариантам их обучения для решения проблем информационной безопасности. Приведены примеры использования и выведены основные направления развития нейронных сетей в области информационной безопасности.

Ключевые слова: *нейронная сеть; криптография; искусственный интеллект.*

APPLICATION OF NEURAL NETWORKS IN THE FIELD OF INFORMATION SECURITY

Orlov Ivan
St. Petersburg State University of Aerospace Instrumentation
Russia, St. Petersburg, str. Bolshaya Morskaya, 67, lit. A
e-mail: like12341@mail.ru

Abstract. The article is devoted to application of neural networks and their training options for solving problems of information security. Examples of the use was given and main directions of development of neural networks in the field of information security was inferred.

Keywords: *neural network; cryptography; artificial intelligence.*

Введение. Наряду с ростом проблем в области информационной безопасности развивается область искусственного интеллекта и компьютерного обучения. Нейронные сети показывают себя чрезвычайно эффективно в распознавании изображений, речи, обработке языка и даже играх, не обходя стороной и область информационной безопасности. Если до недавнего времени еще вставал вопрос об использовании искусственных нейронных сетей для решения проблем защиты информации, то в настоящее время стало ясно, что они переводят эта область на новую ступень развития.

Нейронные сети. Нейронные сети это математическая или компьютерная модель, одна из разновидностей глубокого обучения, симулирующая структурно-функциональный аспект биологических нейронных сетей. Модель обрабатывает информацию, используя искусственно построенные нейроны. Является нелинейным инструментом статистического моделирования, обычно использующимся при моделировании сложных отношений между входными и выходными данными, нахождении взаимосвязей между ними наряду с предсказыванием последующей информации на основе исходной.

В последнее время нейронные сети играют важную роль в решении следующих проблем информационной безопасности:

1) Определение и предотвращение атак на информационные ресурсы;
2) Обнаружение и классификация вредоносного программного обеспечения;
3) Определение вредоносной корреспонденции(спам);
4) Проблемы стеганографии;
5) Генерация псевдослучайных чисел;
6) Биометрический анализ;
7) Обработка текстовых данных на обнаружение “опасной” информации;
8) Полиграфные методы;
9) Криптография и квантовая криптография;
10) и т.д.

Основополагающие критерии при использовании. Время, требуемое для обучения классической нейронной сети, является одним из главных факторов в их использовании на данный момент. Нейронные сети располагаются в виде плотных векторов, операции над которыми, без использования векторизации данных, занимают в разы больше времени. Так, команде из Lenovo Research для обучения малой нейронной сети без использования векторизации, в отличие от нейронной сети, обученной с использованием векторизации(параллельных вычислений), потребовалось в 200 раз больше времени в течение тренировки и в 100 раз больше времени при проведении тестов. Скорость, требуемая для обработки данных для большинства из нейронных сетей, предполагаемо, будет снижаться пропорционально росту количества данных в интернете. Выходом из этого положения могут стать квантовые вычисления, которые, как предполагается, значительно повысить скорость обучения нейронных сетей за счет параллельной обработки данных.

Вероятность ошибки уменьшается, но достичь идеально точного результата на данный момент не предствляется возможности. К примеру, на входной параметр x и целевой параметр y –

установленный заранее положительный результат – обученная нейронная сеть может выдать на выходе ложный ответ о принадлежности параметра x к y. Данный аспект ставит под угрозу системы информационной безопасности, где возникновение ошибки может привести к фатальным последствиям в работе всей системы.

Объем памяти. Память требуется для хранения входных данных, весовых параметров и функций активации. Зависит от выбора нейронной сети и уровня ее обучения. Сильно сказывается при обучении глубоких нейронных сетей, так как нейронная сеть увеличивается относительно количества поступаемых данных.

Применение различных видов нейронных сетей. Нейронные сети Конохена. Главным образом используются для кластеризации (объединения) данных и отображения их особенностей. Показывают себя эффективно в решении проблем распознавания, так как имееют возможность обновления или обучения, на основе полученных данных.

Нейронные сети радиально-базисных функций. Зачастую используются для определения атак на информационные ресурсы. Отличаются в прогнозировании временных рядов, классификации и осуществлении нелинейных отображений. Коренным отличием сетей прежде всего является использование множества переменных одновременно, следовательно, могут быть легко адаптированы под мультисенсорную обработку и слияние полученных данных.

Сверточные нейронные сети. Используются для работы с изображениями, классификация объектов по типам. Основным направлением применения является стеганография. Также были предложены варианты по распознаванию и категоризации вредоносного ПО. Улучшаются с увеличением входных данных сети.

Хаотические нейронные сети. Хаотическая нейронная сеть может предложить значительное понижение требуемого для вычислений объема памяти. Чаще всего используются для шифрования цифрового сигнала, довольно просто расширяется для шифрования двумерных цифровых изображений и трехмерного видео.

Нейронные сети с многослойным перцептроном. Отличаются в решении проблем стохастики, позволяют приближать полученные данные. Могут использоваться в создании моделей по регрессионному анализу. С их помощью строятся эффективные алгоритмы классификации. Зачастую применяются на этапах построения систем с открытым ключом.

Ассоциативные нейронные сети. Сочетают в себе достоинства табличных и комбинационных вычислителей благодаря своей структуре распределенного хранения образов, позволяющей на порядок уменьшить емкость табличных вычислителей. Могут быть эффективно использованы в системах остаточных классов в решении проблем модулярной арифметики на уровне алгоритмов обработки данных и уровне отдельных арифметических операций.

Нейронные сети Хопфилда. Описывают класс асинхронных нейронных сетей, и могут быть использованы в качестве ассоциативной памяти систем. Эти системы показывают возникающие свойства, которые заставляют их сходиться в одно из стабильных, низкоэнергетических состояний системы, независимо от начального состояния системы, называемых аттрактором. Вследствие чего система может иметь произвольные стабильные состояния, представляющие собой содержимое памяти системы. Таким образом, для данного начального состояния или входного значения нейронной сети, нейронная сеть Хопфилда производит выходное значение(аттрактор), которое не может быть определено, имея лишь знания о входном значении сети. Благодаря вышеописанным свойствам нейронная сеть Хопфилда преимущественно используется при построении генераторов псевдослучайных чисел, системах аутентификации и криптоанализе.

Сети долгой-краткосрочной памяти. Имеют преимущество в операциях над последовательными данными. В отличие от основополагающих им рекуррентных нейронных сетей, не имеют проблем с размытием хранимых значений во времени. Хорошо показывают себя в задачах классификации и прогнозировании временных рядов в тех случаях, когда события разделены задержками с неустойчивыми интервалами во времени. Преимущственно находят применение в биометрии в задачах на распознавание речевых и текстовых последовательностей, в определении атак на информационные ресурсы.

Примеры использования. Глубокие нейронные сети сверточного типа, построенные командой из Google, показали 97.84% точность в распознавании номеров домов на фотографиях. Данная сеть была применена к набору данных из ”Street View” изображений, содержащих несколько дессятков миллионов номеров домов. Была достигнута 90% точность в их распознавании. Данная сеть также показала 99.8% точность в reCapcha - одного из самых популярных тестов Тьюринга на распознавание.

В 2010 году был предложен генератор псевдослучайных чисел на основе нейронной сети Хопфилда, воспроизводящей случайные биты с использованием алгоритма SHA-2, который увеличивал непредсказуемость числа на выходе. Полученная последовательность длины 10^6 бит была проверена на стандарте FIPS140-1 и полностью прошла тест. Без использования SHA-2, тесты показывают менее пригодные результаты.

Самый часто используемый протокол для обмена ключами между двумя абонентами - протокол Диффи-Хеллмана. Протокол обмена ключами Neural Key Exchange может стать его заменой, который основывается на синхронизации древовидных машин четности (ДМЧ) – специального типа многослойной нейронной сети прямого распространения. Ожидается, что предполагаемый результат сделает вероятность ошибки минимальной и существенно повысит безопасность данных в системах коммуникации. Является перспективной заменой протокола Диффи-Хеллмана для обычных атак и атак среды квантовых компьютеров, но вероятности взлома, по крайней мере от геометрических атак, генетических алгоритмов и вероятностного анализа, достаточно, чтобы продолжить его совершенствование.

Заключение. Нейронные сети обеспечивают современный подход к большинству направлений в области информционной безопасности. Гораздо успешнее показывают себя в областях нахождения одинаковых свойств исходных данных по заданным параметрам, но и здесь не обходятся без ошибок. Процент возникновения ошибки в работе нейронной сети определяется уровнем ее обучения и, при увеличении количества данных, как правило, уменьшается. Тем не менне, идеально построенных сетей на данный момент нет, что оставляет область использования нейронных сетей в области информационной безопасности, открытой для дальнейших исследований, и на которую в ближайшее время можно возлагать большие надежды.

СПИСОК ЛИТЕРАТУРЫ

1. Червяков Н.И., Галушкин А.И., Евдокимов А.А., Лавриненко А.В., Лавриненко И.Н. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. — М. Издательство: Физмалит, 2012 — 280с.
2. Евдокимов А.А., Тихонов Э.Е. Интеллектуальные информационные системы защиты информации. — Невинномысск. Издательство: НИЭУП, 2012 — 120с.
3. Jan H.P. Eloff, Les Labuschagne, Rossouw von Solms, Gurpreet Dhillon. Advances in Information Security Management & Small Systems Security. — Working Conference on Information Security Management & Small Systems Security September 27–28, 2001, Las Vegas, Nevada, USA — 216с.
4. Harold F. Tipton, Micki Krause. Information Security Management Handbook, Sixth Edition. — CRC Press, 24 июнь. 2009 г. — 392с.
5. Yi Niu, Yichun Peng. Application of Radial Function Neural Network in Network Security. // 2008 International Conference on Computational Intelligence and Security [Электронныйресурс]. URL: http://ieeexplore.ieee.org/abstract/document/4724693/ (дата обращения: 03.09.2017).
6. Tope Komal, Rane Ashutosh, Rahate Roshan, Asst. Prof. S.M. Nalawade. Encryption and Decryption using Artificial Neural Network // International Advanced Research Journal in Science, Engineering and Technology.2015. [Электронныйресурс]. URL: http://www.iarjset.com/upload/2015/april-15/IARJSET%2019.pdf (дата обращения: 02.09.2017).
7. Daniel Socek, Dubravko Culibrk. On the Security of a Clipped Hopfield Neural Network-Based Cryptosystem.29 янв. 2008г. [Электронный ресурс]. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.125.9081&rep=rep1&type=pdf(дата обращения: 12.08.2017).
8. Paweł Kobojek, Khalid Saeed. Application of Recurrent Neural Networks for User Verification based on Keystroke Dynamics // Jounal of telecommunications and information technology. 3 март. 2016. [Электронный ресурс]. URL: http://www.covert.io/the-definitive-security-datascience-and-machinelearning-guide/(дата обращения: 27.08.2017).
9. Ian J. Goodfellow, Yaroslav Bulatov, Julian Ibarz, Sacha Arnoud, Vinay Shet. Multi-digit Number Recognition from Street View Imagery using Deep Convolutional Neural Networks. 14 апр. 2014г. [Электронный ресурс]. URL: https://arxiv.org/pdf/1312.6082v4.pdf (дата обращения: 12.08.2017).
10. Qi Luo. Advancing Computing, Communication, Control and Management. — Springer Science & Business Media, 4 дек. 2009 г. — 290с.
11. Yuhua WangGuoyin WangHuanguo Zhang. Random Number Generator Based on Hopfield Neural Network and SHA-2 (512). [Электронный ресурс]. URL: https://link.springer.com/chapter/10.1007/978-3-642-05173-9_26 (дата обращения: 10.08.2017).
12. Daniel Gibert. Convolutional Neural Networks for Malware Classification. 20 окт. 2016г. [Электронный ресурс]. URL: http://www.covert.io/the-definitive-security-datascience-and-machinelearning-guide/ (дата обращения: 14.08.2017).
13. Prof.Pranita P. Hadke and Prof.Madhuri R. Dubey. Neural Cryptography for Secret Key Exchange // International Journal for Modern Trends in Science and Technology. 3 март. 2016г. [Электронный ресурс]. URL: http://www.covert.io/the-definitive-security-datascience-and-machinelearning-guide/(дата обращения: 20.08.2017).
14. Liew Pol Yee, Liyanage C. De Silva. Application of MultiLayer Perceptron Networks in Public Key Cryptography. 2002г. [Электронный ресурс]. URL: http://ieeexplore.ieee.org/document/1007728/(дата обращения: 25.08.2017).
15. Prof.Pranita P. Hadke and Prof.Madhuri R. Dubey. Neural Cryptography for Secret Key Exchange // International Journal for Modern Trends in Science and Technology. 3 март. 2016г. [Электронный ресурс]. URL: http://www.covert.io/the-definitive-security-datascience-and-machinelearning-guide/(дата обращения: 26.08.2017).

УДК 004.492.3

АНАЛИЗ ПОВЕДЕНЧЕСКИХ СВОЙСТВ СУБЪЕКТА ПРИ АУТЕНТИФИКАЦИИ НА ПРИМЕРЕ РУЧНОЙПОДПИСИ С ИСПОЛЬЗОВАНИЕМ АКСЕЛЕРОМЕТРА

Рудавин Николай Николаевич
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mail: nikolay-rudavin@yandex.ru

Аннотация. В статье проведен обзор основных видов аутентификации и рассказаны преимущества биометрических методов. На основании данного обзора обосновывается выбор для анализа такого перспективного метода биометрической аутентификации, как поведенческая, основанная на индивидуальных особенностях рукописного почерка. Также описан сам прототип,

использовавшийся для анализа биометрических данных и приведены результаты сравнения экспериментальной системы с существующими аналогами. Особенностью рассматриваемого метода является применение акселерометра как ключевого элемента, получающего данные подтверждения личности.

Ключевые слова: *информационная безопасность; биометрическая аутентификация; рукописный почерк; подпись; акселерометр.*

ANALYSIS OF THE BEHAVIOR PROPERTIES OF THE SUBJECT WITH AUTHENTICATION ON THE EXAMPLE OF MANUAL SIGNATURE USING THE ACCELEROMETER

Rudavin Nikolay
St. Petersburg National Research University of Information Technologies. Mechanics and Optics«ITMO»
Russia, St. Petersburg, Kronverksky pr., 49
e-mail: nikolay-rudavin@yandex.ru

Abstract. The article reviews the main types of authentication and tells the advantages of biometric methods. Based on this review, the choice for analysis of such a promising method of biometric authentication, as behavioral, based on individual features of handwriting, is justified. Also, the prototype itself, which was used to analyze biometric data, is described and the results of comparing the experimental system with existing analogues are given. A special feature of the method under consideration is the use of an accelerometer as a key element that receives personal identity data.

Keywords: information security; biometric authentication; handwriting; signature; accelerometer.

Введение. За последнее десятилетие в мире наблюдалось стремительное развитие в сфере электроники и увеличение ее доступности для обычных граждан. Развитие также коснулось и среди программно-аппаратных средств организации несанкционированного доступа казавшиеся ранее надежные средства аутентификации оказались очень уязвимы. В связи с этим проблема поиска новых методов аутентификации оказывается невероятно актуальной.

Особенно актуальными решениями можно считать средства биометрической аутентификации, основанные на поведении субъекта, так как для организации доступа субъекту не требуется наличие дополнительных средств аутентификации, а его биометрические данные невозможно повторить максимально достоверно, так как они основаны не только на физических особенностях субъекта, но и психологические особенности, которые в сочетании с знаниями субъекта о предоставляемой биометрической информации дают максимально эффективный результат для защиты личных биометрических данных. Одним из наиболее перспективных методов динамической аутентификации можно считать получение биометрических данных субъекта по рукописному почерку с применением средств динамической обработки подписи. В результате динамической обработки данные оказываются более защищенными от копирования, чем статические. Данный метод признан заменить устаревшие и малонадежные методы аутентификации такие как PIN-код или пароль и бесконтактная карта или маркерный жетон.

Основная часть. Базовый принцип аутентификации в большинстве случаев следующий: субъект (человек, устройство или программа) предоставляет данные подтверждения себя в виде массива данных произвольной длины, которые преобразуются путем хеширования в защищенные данные, которые будут храниться в базе данных. В дальнейшем последовательность, предоставляемая субъектом будет использоваться как ключ, применяемый в хеш-функции, в случае успешного получения необходимой последовательности личность подтверждается [1]. По виду предоставляемых данных аутентификации существуют три базовых вида подтверждения личности:

1) По PIN-коду или паролю, где последовательностью-ключом для хэш-функции является непосредственно вводимая субъектом информация. Данная система отличается простотой в реализации ввиду отсутствия дополнительных средств преобразования данных для аутентификации, однако для надежности системы должен применяться длинный ключ с большим алфавитом, что может значительно ухудшить доступность к системе.

2) Бесконтактные карты или маркерные жетоны, где маркерный жетон или карта реагирует на сигнал запросного устройства, передавая в ответ индивидуальный кодовый сигнал. Этот сигнал воспринимается запросным устройством и проверяется системой контроля доступа. Если система опознает этот сигнал, личность подтверждается. В этом случае последовательность записана непосредственно на карте или маркерном жетоне, это существенно упрощает скорость процедуры аутентификации, но может ухудшить надежность из-за возможности хищения данных в случае кражи карты или копировании сторонним бесконтактным считывателем, также субъект для доступа на объект постоянно обязан иметь при себе данную карту или жетон, кража или утрата которого подвергает систему угрозе.

3) Аутентификация по биометрическим данным: на основе сопоставления некоторых физиологических характеристик, таких как дактилоскопический узор пальцев, снимок сетчатки глаза, голос, данные поведения субъекта с их образом, хранящимся в базе данных [2].

Исходя из особенностей всех видов аутентификации видно, что биометрическая может применяться в системах с высоким требованием к пропускному режиму и более быстрому доступу, чем при вводе сложного пароля, также в системах, где помимо доступа требуется идентификация субъекта. Отсутствие специальных требований к субъекту, таких как ношение электронного ключа или необходимость запоминания пароля также являются одним из главных преимуществ биометрических методов аутентификации.

В зависимости от вида способа получения подтверждения личности по личностным характеристикам субъекта следует различать статические и динамические биометрические характеристики.

Так, например, в системе обработки подписи, где для снятия данных используется сенсорный экран-планшет обрабатывается только лишь сам рисунок подписи – при этом не учитывается то как субъект ставил подпись в реальном времени, таким образом злоумышленник, получив лишь графическую составляющую подписи может научившись её правильно рисовать обойти систему защиты [3, 4].

В случае же с динамическими биометрическими данных нарушителю будет намного сложнее повторить процедуру подписи, так как учитываются не только положения устройства постановки подписи, но и время, за которое положение изменяется, а также усилие, применяемое субъектом во время движения руки. Для исследования возможности корректной обработки динамической составляющей подписи был собран прототип, состоящий из микроакселерометра и платы-контроллера, обрабатывающей аналоговый сигнал, принимаемый с датчиков перегрузки.

Таблица 1

Технические характеристики элементов акселерометра [5].

Вид элемента:	Микроконтроллер	Акселерометр
Модель	Arduino Nano 2.0	ADXL-335
Размеры платы	42 мм × 18,5 мм	20 мм × 15 мм
Питание	5 В (от USB-mini)	3В
Потребляемый ток	40 мА	0,35 мА
Измеряемые перегрузки	-	+/- 3g
Число аналоговых входов/выходов	8	3
Схема подключения	USB-mini	3V3, GND, A0, A1, A3
Вид передаваемых данных	Дискретные, от 0-1024 с интервалом 10мс	Непрерывные, значения напряжений 0-3 В

Элементы прототипа взаимно совместимы и по своим габаритам позволяют создать устройство-ручку, в которой будет производиться получение биометрических данных и передача в виде цифрового сигнала на устройство обработки данных в реальном времени.

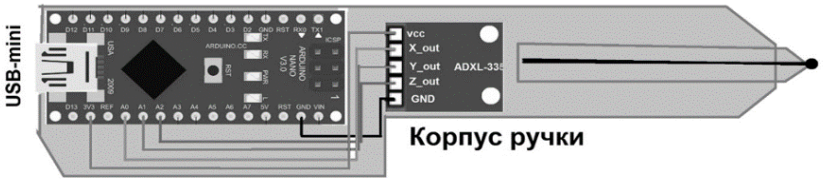


Рис. 1. Компоновка прототипа

Движения человека во время подписи можно образно разделить на горизонтальную плоскость (O:X,O:Y) - непосредственно подпись и вертикальную ось O:Z - постановка ручки в исходное положение и после завершения процедуры подписи.

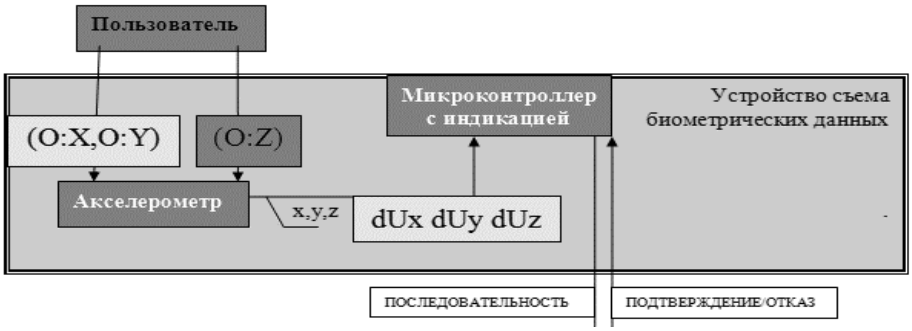


Рис 2. Структурная схема тестовой системы

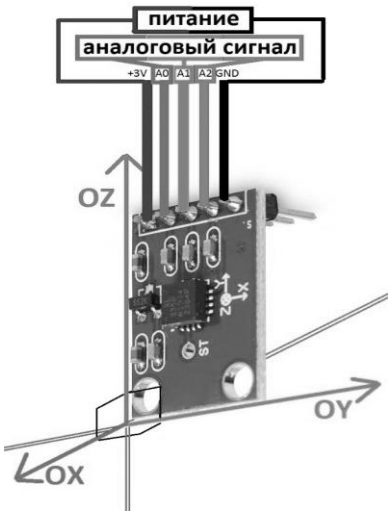


Рис. 3. Схема подключения акселерометра

Информация с контроллера приходит по трем осям в виде разного напряжения на проводах по аналоговым выходам A0, A1 и A3, дополнительно акселерометр запитывается от микроконтроллера через входы 3V3 и GND.

После обработки сигнал в цифровом виде передается на контролируемую зону, где выделяются крайние значения сигналов и их временные интервалы и сверяются с данными имеющимися в базе. На следующем рисунке представлен пример, оцифровки сигнала с частотой дискретизации 10 мс, где на левом рисунке изменение напряжения на аналоговом акселерометре на одной из оси, соответствующие значению перегрузки при движении ручки в одном направлении. Справа – значения цифрового сигнала, соответствующие напряжению: от 0 до 1023 – соответствует минимуму и максимуму измеряемых перегрузок акселерометром [6].

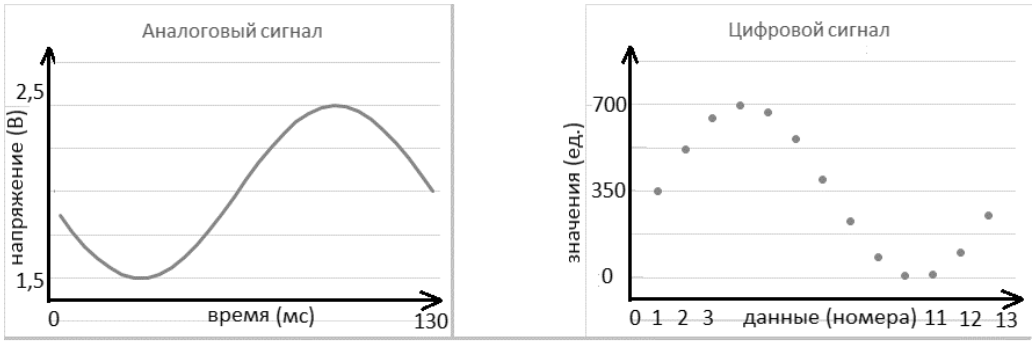


Рис. 4. Оцифровка сигнала по одной из осей

За первичную обработку сигнала отвечает прототип – ручка, на которой размещен акселерометр и микроконтроллер, обрабатывающий сигнал и передающий его на вторичную обработку через USB-порт.

На собранном прототипе удалось собрать данные подписи по двум осям и переданы в программу вторичной обработки сигнала, основная задача которой была найти соответствие между эталонным сигналом и предоставляемым повторно. Для определения соответствия сигнала с эталонным применяется расчет значения коэффициент корреляции Пирсона – Данный критерий позволяет определить, есть ли линейная связь между изменениями значений двух переменных. В статистических расчетах и выводах коэффициент корреляции обычно обозначается как rxy, где x и y – значения последовательностей исходной Y и сравниваемой X [7].

$$r_{xy} = \frac{\sum_{i=1}^{i=n}(d(x_i) \times d(y_i))}{\sqrt{(\sum_{i=1}^{i=n} d^2(x_i) \times \sum_{i=1}^{i=n} d^2(y_i)}}, \quad (1)$$

где rxy - коэффициент корреляции Пирсона; xi, yi - элементы последовательностей X и Y; n - число элементов каждой последовательности; d(xi),d(yi) - разности элемента последовательности и математического ожидания.

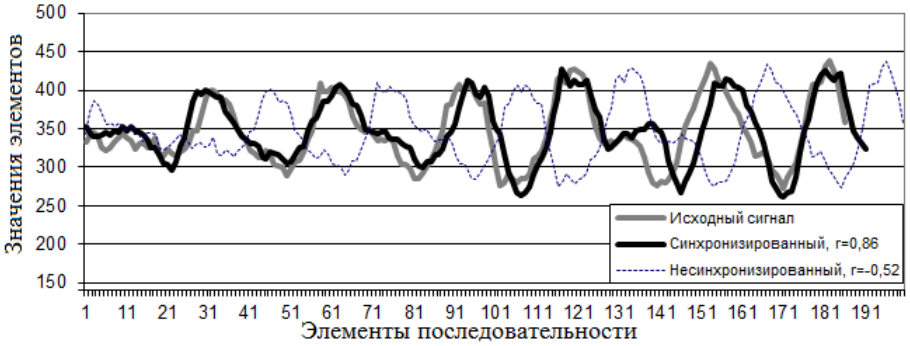


Рис. 5. Визуализация первично обработанного сигнала

На рисунке выше показаны значения коэффициента корреляции (r) оцифрованного сигнала движения руки по одной из осей, видно, что для лучшего соответствия сигнала требуется дополнительнаясинхронизация во времени, таким образом получается высокое значение линейной зависимости сигнала с исходным. В программе вторичной обработки сигнала дополнительная синхронизация добавлена и для проверки работоспособности метода были проведены тесты на проверку значений FRR и FAR – основных показателей надежности в системах биометрической аутентификации, где FRR (False Reject Rate) - ошибка первого рода. Вероятность ошибочного отказа сотруднику, аналогично термину "ложная тревога" в радиолокации, а FAR (False Acceptance Rate) - ошибка второго рода вероятности ошибочного пропуска злоумышленника, аналогично термину "ложная тревога"[8, 9].

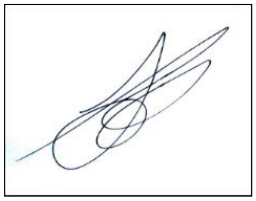


Рис 6. Рисунок эталонной подписи

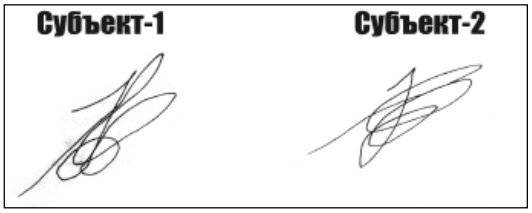


Рис 7. Примеры рисунков подписей, сделанных ложными субъектами

Для начала субъект предоставил свою подпись сделав 100 попыток, далее выбран эталонный коэффициент корреляции, при котором значение FRR=1%. Далее двое ложных субъекта имея рисунок подписи повторяют подпись по 50 попыток каждый, в конечном итоге из 100 попыток подделать подпись удалось пройти аутентификацию 3 раза (FAR=3%).

Таблица 2.

Сравнение результатов тестирования системы с аналогами

Система:	Уровень FRR	Уровень FAR
«Кристалл»	1-3%	1,0%
IBM	0,2%	0,4%
Собственная система	1%	3,0%

Как видно из результатов система незначительно уступает аналогам, что может объясняться отсутствием фильтрации сигнала, которое, в свою очередь упрощает процедуру обработки, тем самым ускоряет работу системы и может применяться в малопроизводительных устройствах. Также для снижения FAR можно увеличить значения допустимого порога по коэффициенту корреляции, а рост значения FRR скомпенсировать применением резервным методом аутентификации – сложный пароль на встраиваемой цифровой клавиатуре.

Заключение.В результате проделанных экспериментов установлена целесообразность продолжения развития системы аутентификации, основанной на обработке динамических биометрических данных рукописного почерка, получаемых аналоговым акселерометром.

В дальнейшем планируется защитить передачу данных между устройством-ручкой и подсистемой обработки биометрических данных путем шифрования. Само же устройство можно

снабдить аккумулятором благодаря низкому энергопотреблению микроконтроллера, таким образом ручка отключается от системы на время процедуры подписи субъектом, а после – подключается обратно, передавая записанные данные уже по зашифрованному каналу связи.

Число свободных аналоговых входов также позволяет применить аутентификацию по pin-коду в качестве резервной, либо делая процедуру подтверждения двухфакторной в зависимости от задачи, которая будет поставлена системе.

Также, имея динамические данные, система в перспективе может оценить надежность предоставляемых биометрических данных по множеству критериев и назначить требования безопасности к подписи клиента - тем самым задав необходимый баланс между доступностью и конфиденциальностью.

СПИСОК ЛИТЕРАТУРЫ

1. Никитин В. В. Существующие системы аутентификации и идентификации пользователей: основные проблемы и направления их модернизации //Вестник Московского университета МВД России. – 2014. – №. 2. – С. 165-172.
2. Гончаров С. М., Боршевников А. Е. Использование технологии высоконадежной биометрической аутентификации в задачах обеспечения безопасности //Проблемы информационной безопасности. – 2016. – С. 195.
3. Лапина Т. И., Лапин Д. В., Петрик Е. А. БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ ПО РУКОПИСНОМУ ПОЧЕРКУ //Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. – 2013. – №. 2. – С. 07-12.
4. Брагина Е. К., Соколов С. С. Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития //Вестник Астраханского государственного технического университета. – 2016. – №. 1 (61).
5. Bora D. J. et al. Novel Approach to Gait Angle Measurement using Tri-axial MEMS Accelerometer //INROADS-An International Journal of Jaipur National University. – 2014. – Т. 3. – №. 1s2. – С. 296-300.
6. Murray-Davis H., Bennett A. Quantitative Analysis of Various Sail Luffing Sensing Methods //Robotic Sailing 2015. – Springer, Cham, 2016. – С. 151-161.
7. Готман А. Ш. Теория вероятностей и математическая статистика //Международный журнал прикладных и фундаментальных исследований. – 2011. – №. 7.
8. Connie T. et al. PalmHashing: a novel approach for cancelable biometrics //Information processing letters. – 2005. – Т. 93. – №. 1. – С. 1-5.
9. Лапина Т. И., Милых В. А., Лапин Д. В. Способ биометрической аутентификации пользователя по рукописному почерку в системах контроля доступа //Информационно-измерительные и управляющие системы. – 2011. – Т. 9. – №. 11. – С. 40-43.

УДК 004.7.056.53

МЕТОДИКИ И ИНСТРУМЕНТЫ АУДИТА СЕТЕВОЙ БЕЗОПАСНОСТИ

Садикова Анастасия Александровна, Титова Юлия Алексеевна, Савков Сергей Витальевич
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: nastya.sadkoo@mail.ru, titova.yulishna@mail.ru, sergsavkov@gmail.com

Аннотация. Со временем сетевая инфраструктура усложняется, расширяются виды приложений и данных. Все эти изменения приводят к тому, что при осуществлении системы информационной безопасности, пользователь может не заметить некоторые уязвимости сети. В связи с этим необходимо проведение регулярного аудита безопасности. В данной статье обобщены виды аудита сетевой безопасности, рассмотрены методологии IAM и SAFETAG, а также особенности их проведения. Приведена краткая характеристика некоторых сканеров уязвимостей. Сделан вывод о том, что, хотя аудит безопасности и носит рекомендательный характер, он является необходимым для обеспечения целостности и конфиденциальности персональных данных людей, так или иначе связанных с организацией.

Ключевые слова: *аудит; тест на проникновение; сканеры уязвимостей; методология аудита; SAFETAG; IAM; сетевая безопасность; международные стандарты безопасности.*

METHODS AND TOOLS OF THE AUDIT OF NETWORK SECURITY

Sadikova Anastasia, Titova Yulia, Savkov Sergei
St. PetersburgNationalResearchUniversity of Information Technologies, Mechanics and Optics «ITMO»
Russia, St. Petersburg, Kronverkskiy pr., 49
e-mails: nastya.sadkoo@mail.ru, titova.yulishna@mail.ru, sergsavkov@gmail.com

Abstract. Over time, the network infrastructure becomes more complicated, expanding the types of applications and data. All these changes lead to the fact that the implementation of the information security system, the user may not notice some network vulnerabilities. In this regard, it is necessary to conduct regular security audit. This article summarizes the types of network security audit reviewed the methodology and IAM SAFETAG, as well as peculiarities of their implementation. A brief description of some of the vulnerability scanners. It is concluded that, although the security audit and is Advisory in nature, it is necessary to ensure the integrity and confidentiality of personal data of people involved with the organization.

Keywords: *audit; penetration testing; vulnerability scanners; audit methodology; SAFETAG; IAM; network security; international security standards.*

Введение. В современном мире сетевая безопасность имеет колоссальное значение. Под сетевой безопасностью понимают комплекс требований, которые предъявляются к инфраструктуре компьютерной сети, при выполнении которых обеспечивается защита сетевых ресурсов от несанкционированного доступа и эффективное функционирование сети в целом.

Одной из задач организации является предоставление своим сотрудникам безопасного доступа к сетевым ресурсам в любое время. Для решения задачи безопасности сети на предприятии проводят аудит сетевой безопасности. В коммерческих организациях руководство озабочено обеспечением безопасности своих активов, поэтому понимает важность проведения аудита. В некоммерческих организациях (далее – НКО) аудиту уделяется намного меньше внимания. Такое пренебрежение чревато тем, что персональные данные граждан, которые по ряду причин обратились в конкретную НКО, а также сотрудников, работающих в данной НКО, могут попасть в руки злоумышленников.

В наше время специалистами используется несколько определений аудита. Но наибольшее распространение получили два из них:

– аудит информационных систем — это проверка используемых компанией информационных систем, систем безопасности, систем связи с внешней средой, корпоративной сети на предмет их соответствия бизнес-процессам, протекающим в компании, а также соответствия международным стандартам с последующей оценкой рисков сбоев в их функционировании;

– аудит информационной безопасности — системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности.

Как видно, суть обоих определений, в общем-то, одинакова и сводится к следующему. Аудит безопасности информационных систем — это их проверка, тестирование, которое должно выявить потенциальные опасности и уязвимости в защите. При этом используется принцип сравнения результатов теста с неким идеалом, установленным целями аудита, а также личным опытом самого аудитора. При этом должно учитываться множество самых разнообразных факторов, в том числе и информация о компании: область её деятельности, размер фирмы и прочее [1]

Целями проведения аудита безопасности являются:

– анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов информационной системы (далее – ИС);

– оценка текущего уровня защищенности ИС;

– локализация узких мест в системе защиты ИС;

– оценка соответствия ИС существующим стандартам в области информационной безопасности;

– выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Существует три вида аудита:

– Активный аудит;

– Экспертный аудит;

– Аудит на соответствие стандартам.

Экспертный аудит можно условно представить,как сравнение состояния информационной безопасности с «идеальным» описанием, которое базируется на следующем:

– требования, которые были предъявлены руководством в процессе проведения аудита;

– описание «идеальной» системы безопасности, основанное на аккумулированном в компании-аудиторе мировом и частном опыте.

При выполнении экспертного аудита сотрудники компании-аудитора проводят следующие виды работ:

– сбор исходных данных об информационной системе, об её функциях и особенностях, используемых технологиях автоматизированной обработки и передачи данных (с учетом ближайших перспектив развития);

– сбор информации об имеющихся организационно-распорядительных документах по обеспечению информационной безопасности и их анализ;

– определение точек ответственности систем, устройств и серверов ИС;

– формирование перечня подсистем каждого подразделения компании с категорированием критичной информации и схемами информационных потоков.

Результаты экспертного аудита могут содержать разноплановые предложения по построению или модернизации системы обеспечения информационной безопасности.

Суть аудита на соответствие стандартам наиболее приближена к тем формулировкам и целям, которые существуют в финансовой сфере — при проведении данного вида аудита состояние информационной безопасности сравнивается с неким абстрактным описанием, приводимым в

стандартах. Официальный отчет, подготовленный в результате проведения данного вида аудита, включает следующую информацию:

– степень соответствия проверяемой информационной системы выбранным стандартам;

– степень соответствия собственным внутренним требованиям компании в области информационной безопасности;

– количество и категории полученных несоответствий и замечаний;

– рекомендации по построению или модификации системы обеспечения информационной безопасности, позволяющие привести её в соответствие с рассматриваемым стандартом;

– подробная ссылка на основные документы заказчика, включая политику безопасности, описания процедур обеспечения информационной безопасности, дополнительные обязательные и необязательные стандарты и нормы, применяемые к данной компании [2]

В данной статье будет более подробно рассмотрен активный аудит сетевой безопасности.

*Активный аудит.*Данный вид аудита является на данный момент одним из самых распространенных. Также его называют инструментальным аудитом. Он заключается в том, что исследование защищенности сети происходит с точки зрения злоумышленника. В процессе данного аудита осуществляется сбор информации о состоянии системы сетевой защиты с помощью программного обеспечения и специальных методов.

При данном виде аудита аудитор ставится на место злоумышленника, владеет минимумом информации (только той, которая находится в открытом доступе). Аудитор в таком случае должен смоделировать как можно больше видов атак на систему сетевой защиты, которые мог бы осуществить хакер. В результате подобного аудита формируется информация об уязвимостях, степени их критичности и методах устранения, а также предоставляются рекомендации по модернизации сетевой защиты. Полнота этой информации зависит от квалификации аудитора и используемых систем анализа защищенности.

Примером активного аудита является Pentest. Тест на проникновение (англ. penetrationtesting, pentest) – один из методов оценки безопасности компьютерных сетей средствами моделирования атаки злоумышленника. Целью такого испытания является оценка возможности проникновения в сеть и прогнозирование экономических потерь в случае удачной атаки.

Чтобы просканировать сеть и ее устройства, обнаружить в ней уязвимости, используют сканеры уязвимостей. Данный вид анализа занимает меньше времени, чем тест на проникновение, а также требует меньше денежных вложений. В результате работы сканера пользователь получает более конкретную и объективную оценку защищенности сети, поскольку сканеры уязвимостей представляют собой программные или аппаратные средства. С помощью сканера можно получить более широкий спектр уязвимостей, чем при использовании теста на проникновение. Получив этот список можно уже разработать план действий по устранению или смягчению этих уязвимостей. Также могут быть использованы низкоуровневые средства, такие как сканер портов, для выявления и анализа возможных приложений и протоколов, выполняющихся в системе [7, 8]

1. Nessus. Чтобы проверить надежность сервисов, можно использовать как стандартные методы, так и имитацию сетевых атак с использованием базы данных. В результате работы Nessus представит отчет, содержащий список уязвимых мест, рекомендации по их устранению и уровень риска для каждого из них. Можно сконфигурировать сканер так, чтобы после первоначального исследования системы в дальнейшем он будет опираться на полученные данные, отмечая только изменения в результатах исследования. Также в данный сканер встроен сканнер портов, который распознает сервисы, причем не по привязке к портам, а с помощью сигнатур, количество которых также может быть расширено. Его отличительной особенностью является то, что данный сканер использует плагины. Полезным свойством сканера становится возможность планирования сканирования заданных хостов, определенных до этого как наиболее важные с точки зрения исследования защищенности. Но есть у него и два недостатка. Первый — при отключенной опции «safe checks» некоторые тесты на уязвимости могут привести к нарушениям в работе сканируемых систем. Второй — цена. Годовая лицензия может обойтись в 114 тысяч рублей [3, 4]

2. OpenVAS – сканер уязвимостей, а также средство управления уязвимостями с открытым исходным кодом. Так же, как и Nessus, использует архитектуру клиент – сервер. Предназначен для активного мониторинга узлов вычислительной сети на предмет наличия проблем, связанных с безопасностью, оценки серьезности этих проблем, а также для контроля их устранения. Активный мониторинг означает, что OpenVAS выполняет какие-то действия с узлом сети: сканирует открытые порты, посылает специальным образом сформированные пакеты для имитации атаки или даже авторизуется на узле, получает доступ к консоли управления, и выполняет на нем команды. Затем OpenVAS анализирует собранные данные и делает выводы о наличии каких-либо проблем с безопасностью. Эти проблемы, в большинстве случаев касаются установленного на узле необновленного ПО, в котором имеются известные и описанные уязвимости, или же небезопасно настроенного ПО.

3. Nmap используется для сканирования хостов и служб в сети. Nmap имеет продвинутые функции, которые могут выявить различные приложения, запущенные на системах, также как службы

и особенности отпечатков ОС. Это один из наиболее широко используемых сетевых сканеров, он является очень эффективным, но в то же время и очень заметным. Nmap рекомендуется к применению в специфичных ситуациях, для предотвращения срабатывания механизма защиты. Если пользователь тестирует на проникновение конкретный компьютер/сервер, то необходимо проверить все порты — с первого до последнего (65535) [4].

Примеры стандартов, на соответствие которым проводится аудит безопасности:

– ISO 27000 – Международные стандарты управления информационной безопасностью – это семейство включает в себя Международные стандарты, определяющие требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению;

– ISO 15408 – Общие критерии оценки безопасности информационных технологий – содержат обобщенное формализованное представление знаний и опыта, накопленного в области обеспечения информационной безопасности на протяжении десятилетий;

– ISO 18028 – Международные стандарты сетевой безопасности – Этот стандарт содержит руководство по созданию сетей и организации взаимодействия с учетом аспектов безопасности при соединении сетей между собой и при получении удаленного доступа к сети. Руководство включает идентификацию и анализ факторов, связанных с сетевыми взаимодействиями, которые следует принимать во внимание при определении требований к сетевой безопасности, идентификация необходимых областей контроля при подключении к сетям и обзор возможных областей контроля, включая проектирование и внедрение;

– BSI\IT Baseline Protection Manual – Немецкий стандарт «Руководство по обеспечению безопасности ИТ» – содержательный и практичный стандарт по информационной безопасности. Он представляет собой набор документов, в которых содержатся подробные руководства по обеспечению информационной безопасности применительно к различным аспектам функционирования ИС и различным областям ИТ. Данный стандарт постоянно совершенствуется с целью обеспечения его соответствия текущему состоянию дел в области ИТ и информационной безопасности. К настоящему времени накоплена уникальная база знаний, содержащая информацию по угрозам и контрмерам в хорошо структурированном виде.

Методология IAM. Для оценки сетевых систем правительства Соединенных Штатов Америки Агентство Национальной Безопасности разработала методологию The INFOSEC Assessment Methodology, или IAM. Данная методология сейчас используется как государственными, так и негосударственными организациями. Целью IAM проекта является оказание помощи предприятию в улучшении позиции ее службы информационной безопасности. Оценка проводится в три этапа.

На первом этапе проводится оценка системы управления информационной безопасностью. На втором этапе – технологический аудит защищенности. Третий этап представляет собой анализ информационных рисков.

Отличительной особенностью IAM является то, что данная методология не просто содержит набор определений и требований, в ней описан процесс подготовки к оценке, непосредственный процесс выполнения оценки и описание документирования проекта. Есть 3 категории и 18 классов в рамках этих категорий, которые должны быть обязательно оценены в процессе тщательной IAM оценки, которая проводится на втором этапе. Этими категориями являются:

– Категория управления: 4 класса (например, планирование на случай чрезвычайных ситуаций и управление конфигурацией);

– Техническая категория: 9 классов (например, аутентификация, контроль подключений к сети);

– Категория операций: 5 классов (например, маркировка, образование и обучение).

Одной из целей аудита является проверка на соответствие стандартам. Если в организации необходимо проведение данного вида аудита, то IAM является подходящей ступенью в подготовке к подобной деятельности [5]

Методология SAFETAG. Традиционный аудит сетевой безопасности основывается на предположении о том, что организация имеет время, деньги, а также возможность стремиться к как можно более полной безопасности. К сожалению, это непозволительная роскошь для малых компаний. Именно поэтому международной организацией Internews была разработана SAFETAG (Security Auditing Framework and Evaluation Template for Advocacy Groups) – методология аудита цифровой безопасности для НКО. Аудит SAFETAG состоит из нескольких шагов по сбору информации и подтверждению, а также научно-исследовательских мероприятий с сотрудниками, организованные для сбора задач, каждая из которых поддерживает основные цели SAFETAG, создавая оценку риска при одновременном наращивании потенциала организации. Отличительной особенностью этой методологии является то, что она распространяется по лицензии Creative Commons и имеет открытый исходный код. Мероприятия и структура SAFETAG показаны на рис. 1 и рис. 2.

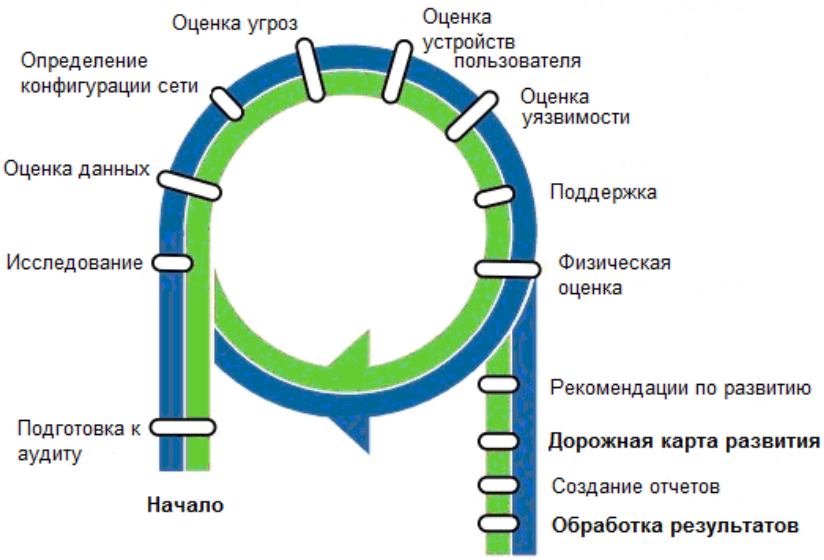


Рис. 1. Мероприятия SAFETAG

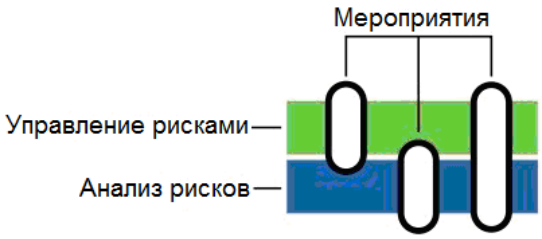


Рис. 2. Структура SAFETAG

В процессе работы аудитор сначала подготавливает необходимые технические компоненты аудита, затем фокусируется на непосредственном наблюдении за организацией и ее инфраструктурой. Эта фокусировка состоит из пассивной разведки публично доступных источников данных. Данная деятельность необходима для определения общедоступных ресурсов, связанных с компанией, и сбора информации об этих ресурсах.

На следующем этапе определяются конфиденциальные данные организации, места их хранения, а также способы передачи. Далее происходит идентифицирование сетевых устройств хоста; услуг, которые используются этими устройствами, а также средства защиты этих устройств. Следующий компонент использует разнообразные мероприятия по выявлению возможных атак и сбору справочной информации о способности этих атак поставить под угрозу деятельность организации. Компонент «Оценка устройств пользователя» позволяет аудитору оценить безопасность отдельных устройств сети путем интервью, обзора и осмотра этих устройств. За счет тестирования работы сети против различных онлайн и оффлайн ресурсов, таких как база данных уязвимостей, появляется возможность обнаружить недостатки устройства предприятия. Также аудитор оказывает необходимую помощь, такую как исправление инструментов, консультирование по вопросам будущих проектов.

В течение этапа «Физическая оценка» аудитор анализирует потенциальные риски, связанные с физическим доступом, хранением, резервным копированием и шифрованием цифровых данных, а также предлагает новые политики безопасности и практики. Далее определяются сильные и слабые стороны компании к принятию новых методов цифровой и физической безопасности; новые введения, которые организация могла бы принять к сведению после обнаружения уязвимостей. «Дорожная карта развития» представляет собой сортировку рекомендаций в отношении организации, а также угроз и возможностей. Аудитор взвешивает затраты на реализацию этих рекомендаций, а затем создает оптимальную дорожную карту для предприятия. Далее создается отчет, в котором указаны замечания к рекомендациям, а также в нем содержится информация о текущем состоянии безопасности. На этапе «Обработка результатов» аудитор получает обратную связь о своем докладе, а также оценивает успешность процесса с течением времени через постоянные переговоры с компанией [6].

Заключение. Аудит как средство защиты информации носит сугубо рекомендательный характер, другими словами, эта процедура не привносит изменений в саму систему. Однако анализ полученных данных позволяет говорить о мерах защиты от несанкционированного доступа к

конфиденциальным ресурсам. Сканеры безопасности охватывают довольно обширную сферу проблем, поэтому благодаря их использованию можно не только искать уязвимые прог

раммы в сети, но и изменять политику безопасности, реагируя на обнаруженные проблемы [7]. При планировании проверки состояния системы информационной безопасности важно не только точно выбрать вид аудита, исходя из потребностей и возможностей компании, но и не ошибиться с выбором исполнителя. Результаты любого вида аудита содержат рекомендации по модернизации системы обеспечения информационной безопасности. Если аудит проводит консалтинговая компания, которая кроме консалтинговой деятельности занимается еще и разработкой собственных систем защиты информации, она, по понятным причинам, заинтересована в том, чтобы результаты аудита рекомендовали организации использовать её продукты. Для того чтобы рекомендации на основе аудита были действительно объективными, необходимо, чтобы компания-аудитор была независима в выборе используемых систем защиты информации и имела большой опыт работы в области информационной безопасности [9].

СПИСОК ЛИТЕРАТУРЫ

1. Кравчук Д. И., Коркушко Д. А. Аудит безопасности корпоративных информационных систем // Молодой ученый. — 2015. — №10. — С. 697-700.
2. Просянников Р. Виды аудита информационной безопасности // Журнал «Connect!». 2004. №12. [Электронный ресурс]. – Режим доступа: http://www.bre.ru/security/24272.html, свободный, Яз. рус. (дата обращения 07.01.2017)
3. Сетевые сканеры безопасности: возможности, принцип работы и передовые решения. [Электронный ресурс]. – Режим доступа: http://www.kp.ru/guide/setevye-skanery-bezopasnosti.html, свободный. Яз. рус. (дата обращения 26.12.2016)
4. Милосердов А. В., Гриднев Д. А. Тестирование на проникновение с помощью KaliLinux 2.0.: WebWare, 2015. – 348 с.
5. Officialpage «SystemExperts». [Электронный ресурс] — Режим доступа. — URL: https://systemexperts.com/, свободный, Англ. яз. (дата обращения 26.12.2016).
6. Officialpage «SAFETAG». [Электронный ресурс] — Режим доступа. — URL: https://safetag.org/# , свободный, Англ. яз.(дата обращения 26.12.2016).
7. Обзор бесплатных инструментов для аудита web-ресурсов и не только. [Электронныйресурс]. – Режим доступа: https://habrahabr.ru/post/125206/ , свободный. Яз. рус. (дата обращения 26.12.2016)
8. Лучшие инструменты пен-тестера: сканеры безопасности. // Журнал «Хакер». 2010. [Электронный ресурс]. – Режим доступа: https://xakep.ru/2010/04/13/51777/, свободный. Яз. рус. (дата обращения 26.12.2016)
9. Аудит безопасности: когда и чем проводить? // CNews – Издание о высоких технологиях. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/articles/audit_bezopasnosti_kogda_i_chem_provodit_, свободный, Яз. рус. (дата обращения 26.12.2016).

УДК 004.056.5

ПОВЫШЕНИЕ ТОЧНОСТИ МЕТОДОВ СТЕГАНОАНАЛИЗА ПУТЕМ ОПТИМИЗАЦИИ ПАРАМЕТРОВ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

Сивачев Алексей Вячеславович, Михайличенко Ольга Викторовна
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: sivachev239@mail.ru , crypto_ifmo@mail.ru

Аннотация. В докладе рассмотрена задача обнаружения факта встраивания в область дискретного вейвлет-преобразования и рассмотрены причины недостаточной эффективности современных методов стеганоанализа. Показано, что причина недостаточной эффективности современных методов стеганоанализа связана с большой степенью разброса используемых для обнаружения встраивания параметров, составляющих опорный вектор. По итогам исследования в докладе предложена методика, позволяющих улучшить эффективность современных методов стеганоанализа с помощью специализированного вейвлета.

Ключевые слова: *стеганография, методы стеганоанализа, бинарная классификация, дискретное вейвлет-преобразование.*

INCREASE OF ACCURACY OF STEGOANALYSIS METHODS BY OPTIMIZING PARAMETERS OF WAVELET-TRANSFORMATION

Sivachev Alexey, Mikhailichenko Olga
St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverkskiy pr., 49
e-mails: sivachev239@mail.ru , crypto_ifmo@mail.ru

Аннотация. This report deals with problem of detecting the fact of embedding into the wavelet transform domain. This article shows the reasons of low efficiency of modern methods of steganoanalysis. It is shown that the reason for low efficiency of modern methods of steganoanalysis is associated with a high dispersion of the parameters used to detect the embedding. According to the results of the research, the article suggests a technique that allows improving the efficiency of modern methods of steganoanalysis using a specialized wavelet.

Ключевые слова: *steganography, methods of steganalysis, binary classification, discrete wavelet transformation.*

На сегодняшний день существует и находит широкое применение большое количество методов скрытия информации в цифровых изображениях с использованием стеганографии. Значительный прогресс наблюдается в области разработки стеганографических методов вейвлет (ДВП) области встраивания. Увеличение интереса к встраиванию информации в область ДВП изображения связано с распространением формата сжатия изображений JPEG 2000, который основан на использовании ДВП.

Для противодействия противоправному использованию стеганографии [2] на сегодняшний день разработаны методы стеганоанализа, которые должны выявлять факт стеганографического встраивания в область дискретного вейвлет-преобразования цифровых изображений. Множество современных методов стеганоанализа в области ДВП основаны на методах машинного обучения. На сегодняшний день не существует универсальных методов стеганоанализа, которые позволяли бы однозначно определить факт встраивания в цифровое изображение [2].

Точность обнаружения встраивания в область ДВП на сегодняшний день не позволяет гарантировать абсолютную успешность пассивного противодействия с их применением. Например, авторы метода [3] приводят данные по точности разработанного ими метода, согласно которым наилучшая точность метода [3] составляет 80% корректно классифицированных изображений при 20% объеме встраивания от максимального объема встраивания. Т.е. около 20% изображений классифицируются неверно. В случае снижения объема встроенной полезной нагрузки процент корректных результатов скорее всего еще более снизиться, а некорректных результатов соответственно возрастет. Таким образом исследования направленные на повышение точности обнаружения факта встраивания в область ДВП изображения являются актуальными.

Исследование предметной области. Многие из существующих методов стеганоанализа, например, методы [3-5], основаны на использовании значений статистических моментов областей коэффициентов LL, HL, LH, HH, получаемых при дискретном вейвлет-преобразовании изображения в качестве основы для вектора параметров, используемых в последствии для классификации изображений с использованием методов машинного обучения.

Как показали исследования стеганографическое встраивания оказывает заметное влияние на значения данных статистических моментов, однако значения данных статистических моментов обладают заметным разбросом значений, что приводит к тому, что приводит к тому, что множества значений статистического момента для оригинальных и для стего изображений имеют значительную область пересечения.

Значительное пересечение множеств значений для оригинальных и стего изображений не позволяет однозначно классифицировать изображение как оригинальное или стего изображение с использование данных статистических моментов. Исследования показывают, что степень пересечения множеств значений статистических моментов для оригинальных и стего изображений зависит от набора низко- и высокочастотных коэффициентов, используемых для дискретного вейвлет-преобразования.

Зависимость между степенью пересечения множеств значений статистических значений для оригинальных и стего изображений и используемым вейвлетом позволяет подобрать специализированный вейвлет, который позволит уменьшить область пересечений для множеств значений оригинальных и стего изображений, либо подобрать специализированный вейвлет который оценить погрешность значений статистических моментов. На основании выявленной зависимости можно предложить методику, которая позволит повысить эффективность использования статистических моментов, что позволит повысить эффективность современных методов стеганоанализа.

СПИСОК ЛИТЕРАТУРЫ

1. SPYCRAFT: The Secret History of the CIA’s Spytechs from Communism to Al-Qaeda [Электронныйресурс]: Central Intelligence Agency – Режимдоступа: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol52no2/spycraft-the-secret-history-of-the-cia2019s.html (Датаобращения 05.03.2017)
2. Prokhozhev N., Mikhailichenko O., Sivachev A., Bashmakov D., Korobeynikov A.G. Passive Steganalysis Evaluation: Reliabilities of Modern Quantitative Steganalysis Algorithms [Текст], Advances in Intelligent Systems and Computing. 2016. Vol. 451. pp. 89-94.
3. Gireesh Kumar T., Jithin R., Deepa D. Shankar Feature Based Steganalysis Using Wavelet Decomposition and Magnitude Statistics [Текст],Advances in Computer Engineering (ACE), 2010, pp. 298-300
4. Farid Hany Detecting Steganographic Messages in Digital Images [Текст], Technical Report TR2001-412, Dartmouth College, Computer Science Department, 2001
5. Changxin Liu, Chunjuan Ouyang, Ming Guo, Huijuan Chen Image Steganalysis Based on Spatial Domain and DWT Domain Features[Текст], Proceedings of the 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing - Volume 01, pp. 329-331

УДК 004.72

ПРОБЛЕМА АНОНИМНОСТИ В СЕТИ ИНТЕРНЕТ. СРАВНЕНИЕ МЕТОДОВ АНОНИМИЗАЦИИ ПОЛЬЗОВАТЕЛЯ

Титова Юлия Алексеевна, Садикова Анастасия Александровна, Савков Сергей Витальевич
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: titova.yulishna@mail.ru, nastya.sadkoo@mail.ru, sergsavkov@gmail.com

Аннотация. Сейчас все большее количество людей беспокоит проблема анонимности в сети Интернет. К сожалению, полностью обезопасить себя нельзя, однако, используя методы анонимизации, риски можно свести к минимуму. В статье рассмотрены самые популярные методы, позволяющие обеспечивать анонимность и информационную безопасность в сети Интернет, такие как различные Proxy-серверы, VPN-серверы, сети Tor, I2P, и метод «крышевания» доменов. Рассмотрен принцип их работы, проанализированы основные преимущества и недостатки. Сделаны выводы, что каждый метод разработан для определённых целей, а значит, при выборе способа анонимизации следуют руководствоваться конкретными задачами, которые стоят перед пользователем.

Ключевые слова: *анонимизация; proxy-сервер; VPN; Tor; I2P.*

THE PROBLEM OF ANONYMITY IN THE INTERNET NETWORK. COMPARISON OF METHODS OF USER ANONYMIZATION

Titova Yulia, Sadikova Anastasia, Savkov Sergei
St. Petersburg National Research University of Information Technologies, Mechanics and Optics «ITMO»
Russia, St. Petersburg, Kronverkskiy pr., 49
e-mails: titova.yulishna@mail.ru, nastya.sadkoo@mail.ru, sergsavkov@gmail.com

Abstract. Nowadays more and nore people are concerned about the problem of anonymity on the Internet. Unfortunately, one cannot completely protect onerself, however, using anonymization methods, risks can be minimized. The article covers the most popular methods that allow anonymity and information security on the Internet, such as various Proxy servers, VPN servers, Tor networks, I2P, and the method of domain "fronting". The principle of their work is considered, the main advantages and disadvantages are analyzed. It is concluded that each method is designed for certain purposes, and therefore, when choosing the method of anonymization, one should follow specific tasks that are faced to the user.

Keywords: *anonymization; proxy-server; VPN; Tor; I2P.*

Введение. Ведущие специалисты в области информационной безопасности утверждают, что полной анонимности в сети Интернет добиться практически невозможно. Поэтому среднестатистический пользователь, считающий себя анонимом, является таковым лишь формально. Словарь Ожегова даёт следующее определение слову анонимность: Без указания имени того, кто пишет, сообщает о чем-либо [1]. Действительно, пользователи сети Интернет стараются не указывать свои личные данные на подозрительных сайтах, однако это не гарантирует анонимности в сети. Большинство Web-серверов ведёт контроль посещаемости, а значит IP адреса устройств, с которых был выполнен вход на сайт, остаются в базе данных, где также фиксируется активность пользователя на сайте. Помимо этого, задействуются социальные сети. Так, к примеру, по официальным данным, Facebook, MySpace и несколько других социальных сетей продавали личные данные рекламным компаниям, которые в дальнейшем использовали их для поиска имён потребителей, контактных данных и другой личной информации [2]. Таким образом, осуществляется взаимодействие сайтов, в процессе которого происходит обмен информацией и составление полноценной характеристики о каждом клиенте. Более продвинутые пользователи пытаются оградить себя от этого и прибегают к различным изобретательным подходам для достижения анонимности. Но это им не всегда удается, поскольку в настоящее время со стороны, как государства, так и частных организаций активно ведется борьба с анонимностью в сети Интернет. Принимаются меры по деанонимизации: устанавливаются обязательная идентификация пользователей при использовании общественных точек доступа, блокируются proxy-серверы и анонимные сети, контролируется трафик с помощью технологии
DPI и пр.

Методы анонимизации зачастую используются злоумышленниками, с целью избежать наказания за правовые нарушения. В борьбу с ними вступают правоохранительные органы, которые при помощи способов деанонимизации устанавливают реальную личность преступника, его место нахождения, активность в сети Интернет и прочую необходимую информацию.

В этом и заключается проблема анонимности в сети Интернет. Всегда будут люди, которые хотят защитить информацию о себе. А в противовес им будут существовать организации, которые пытаются извлечь выгоду из обладания личными данными пользователей, и правоохранительные

органы, задача которых деанонимизировать и наказать правонарушителя. Поэтому способы анонимизации в сети интернет будут рассмотрены с различных позиций.

Работа Proxy-серверов.

Одним из самых распространённых методов анонимизации является использование Proxy-серверов. Основным идентификатором в сети является IP адрес. Он служит обратным адресом, на который приходит ответ от Web-сервера. Поэтому избавиться от IP невозможно. Но с помощью Proxy-сервера его можно заменить.

Общий принцип работы таких методов заключается в появлении между пользователем и сетью Интернет связующего звена. Proxy-сервер получает запрос от клиента и перенаправляет его уже со своим IP адресом на Web-сервер. На рис. 1. представлена принципиальная схема работы Proxy-сервера. Таким образом у Web-сервера имеется адрес только Proxy-сервера. Ответ также проходит через Proxy-сервер и направляется обратно пользователю.

С точки зрения обеспечению анонимности различают три основных вида Proxy-серверов: HTTP(S) Proxy, CGI Proxy и Socks Proxy. HTTP(S) Proxy являются самыми распространёнными. Они позволяют скрыть IP пользователя, но в передаваемом трафике указывают, что был использован Proxy-сервер. Ещё одним недостатком такого сервера является работа только для HTTP протокола. Следующий вид это CGI Proxy, которые также называют анонимайзерами.

Пользователь Proxy-сервер Сеть Интренет

Рис. 1. Принципиальная схема работы Proxy-сервера

Они привязаны к браузеру и представляют собой Web-сервер, в поле которого пользователь вводит URL. CGI Proxy выгружает запрашиваемую страницу себе, и пользователь может её посмотреть на сайте Proxy-сервера. Другой вид серверов это Socks Proxy. Они действуют по общему принципу, однако у них есть одно кардинальное отличие. Обмен информацией пользователь – proxy-сервер происходит с помощью специальных протоколов (socks4, socks5). В этом случае IP адрес клиента вообще не используется. Выявить такой сервер затруднительно, поскольку передаваемая информации проходит через него без изменений и не содержит в себе никаких данных об использовании связующего звена. Также стоит упомянуть о цепочках Proxy. Для их создания необходимы специальные программы, которые позволяют объединить сервера в так называемый виртуальный туннель и передавать по нему информацию от пользователя к конечному Web-серверу. При создании туннеля можно использовать Proxy-сервер одного вида или комбинировать их [3]. Однако цепочка Proxy-серверов считаются неэффективными, ввиду того, что в неё содержится информация обо всех серверах, которые в неё входят. Отличие заключается лишь в том, что для деанонимизации возникает необходимость получить ответ от каждого Proxy-сервера этой цепочки.

Основным недостатком такого метода является то, что протоколы всех действий хранятся на Proxy-серверах. Их владельцы могут подменить информацию или даже продать. Поэтому важно, пользоваться только надежными серверами. Если все же сервер надёжный, вычислить, что пользователь является анонимом, можно по cookies. Это происходит путём сравнивания данных cookies до использования proxy-сервер с новыми данными. Если cookies совпадают, а IP адреса различаются, сервер делает выводы и заносит данный адрес в чёрный список. Proxy-серверы не используют дополнительных методов шифрования, поэтому считается, что они не могут обеспечивать высокий уровень безопасности. Также на некоторых сайтах устанавливаются специальные java-скрипты, которые позволяют установить реальный IP адрес пользователя. Таким образом наиболее популярные серверы вычисляются и блокируются.

Работа VPN-серверов.

Следующий способ анонимизации, который будет рассмотрен, это VPN – Virtual Private Network. Такая логическая сеть организуется поверх другой сети, в общем случае поверх сети Интернет. По аналогии с Proxy-серверами трафик, поступающий от пользователя, проходит через частную сеть и, поступая на заданный Web-сервер, уже имеет IP адрес VPN-сервера. Тем самым пользователь скрывает свой реальный IP. Принципиальную схему работы VPN-сервера можно увидеть на рис.2. Преимуществом такого способа является шифрование. С помощью, установленной на компьютер программы, весь исходящий трафик скрывается с помощью выбранного алгоритма, и в зашифрованном виде передаётся на VPN-сервер. Далее на сервере информация дешифруется и передаётся адресату.

Рис. 2. Принципиальная схема работы VPN-сервера

Недостатки этого способа во многом схожи с рассмотренными ранее. Однако, в отличает от Proxy-серверов, способ VPN обеспечивает зашифрованный туннель между пользователем и VPN-сервером [4]. Это не гарантирует полной безопасности, поскольку на выходе из VPN-сервера трафик расшифровывается и, передаваясь в таком виде, он может быть перехвачен. Чтобы избежать этого, дополнительно используют SSL и TLS. Это криптографические протоколы, используемые для создания двустороннего защищенного канала. Они обеспечивают конфиденциальность, обнаружение подмены и аутентификацию узлов.

Работа сети Tor.

Более совершенный метод анонимизации представляет Tor. Его принципиальная схема работы представлена на рис. 3. Это программное обеспечение, осуществляющее распределение трафика по различным серверам с использованием так называемой «луковой» маршрутизации. Узлами системы Tor, помимо специальных серверов являются и устройства самих пользователей. В такой системе реализовано ступенчатое шифрование. Случайным образом выбирается количество промежуточных узлов. Затем производится соединение с каждым из них и передаётся личный ключ (для каждого узла свой). Многократно зашифрованные данные передаются на первый узел, который с помощью своего личного ключа открывает последний уровень шифрования и получает адрес следующего узла [5]. Следующий узел делает то же самое – расшифровывает очередной «слой» и, получив адрес, отправляет дальше. При этом на промежуточных звеньях передаваемая информация и конечный адресат являются невидимыми. Это обеспечивает отсутствие прямых связей. Завершающий узел цепочки Tor передаёт сообщение в сеть. Таким образом источник информации скрывается и запутывает обратный путь.

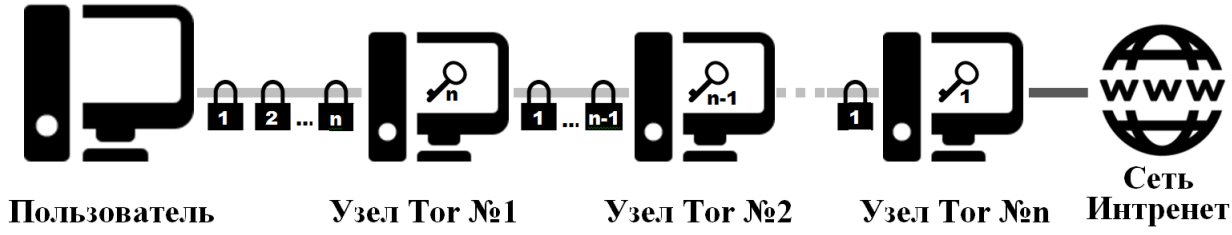


Рис. 3. Принципиальная схема работы сети Tor

В случае использования Tor следует разделять понятия анонимности и безопасности передаваемых данных, поскольку Tor позволяет защищать данные только внутри своей сети, а между конечным звеном и сетью Интернет такой защиты уже нет [6]. К примеру, даже на выходном узле цепи информация может подвергаться изменениям и мониторингу. Несмотря на это данный метод считается одним из наиболее эффективных способов анонимизации. Также сеть Tor имеет свои внутресетевые Web-сайты - onion сайты, доступные только внутри сети Tor. Это значит, что при пользовании внутренней сетью обеспечивается почти максимальная анонимизация. Более того, значительное преимущество Tor заключается в том, что заблокировать цепочку практически невозможно. Это обусловлено тем, что для блокировки Tor придётся блокировать целую подсеть, так как узлами цепи, помимо серверов являются и устройства пользователей. Кроме того, следует отметить, что цепочка узлов, по которым передаётся трафик, является динамической. Она меняется через определённые промежутки времени. Несмотря на это анонимность, достигнутую с помощью рассмотренного способа, нельзя считать абсолютной, потому как на эту систему являются действенными атаки с использованием межсайтового скриптинга.

Комбинация Tor и VPN.

Для устранения утечек информации на входном и выходном узле цепочки Tor используются комбинации методов VPN и Tor. Существует два способа комбинации. Первый – когда VPN-сервер стоит перед сетью Tor в качестве входного узла. В этом случае трафик, поступающий на первый узел цепочки Tor, имеет IP адрес только VPN-сервера. Также эта комбинация позволяет скрыть от Интернет-провайдера сам факт использования системы Tor. И второй – где VPN-сервер используется в качестве выходного узла. Такой способ позволяет избежать прослушивания трафика на последнем узле цепочки Tor. Однако методом анализа выходной узел может выявить использование VPN-

сервера, поскольку клиент будет обращаться только к одному IP адресу. Несмотря на это, данные комбинации считаются неэффективными по сравнению с сетью Tor. Поскольку с применением данных комбинаций возникают дополнительные угрозы утечки данных с VPN-сервера.

Работа сети I2P.

Схожим по некоторым параметрам методом является построение сети I2P – Invisible internet project. В нём используется «чесночная» маршрутизация. Каждое сообщение многократно шифруется, как в описанной ранее «луковой». Затем объединяется с транзитными сообщениями в один пакет и передаётся по выстроенному туннелю. Когда же пользователю приходит пакет, он открывает его своим личным ключом и получает только адресованные ему сообщения. Остальной пакет является недоступным, потому как по отношению к нему пользователь лишь промежуточное звено [7]. Таким образом, пакет пересылается далее от узла к узлу. В отличие от сети Tor, маршруты Клиент – Web-сервер и Web-сервер – Клиент содержат разные узлы.

На рис.4. изображена принципиальная схема построения маршрутов в сети I2P. Исходящий туннель позволяет скрыть данные об отправителе, а входящий – о получателе. Для связи этих туннелей используется сетевая База NetDb, в которой хранятся маршрутные данные клиентов. Следует отметить, что сеть I2P имеет свою адресацию. К каждому узлу привязывается, генерируемый случайным образом, I2P адрес, вместо IP, который используется в сети Интернет. IP адресом в такой цепи обладает только выходной узел, который обеспечивает связь с глобальной сетью. Вследствие этого узнать IP адрес пользователя весьма затруднительно. Также анонимность внутри сети обеспечивается за счёт того, что в ней не используется привычный DNS-сервер. Вместо него у каждого пользователя есть обновляемая адресная книга, в которой записаны доменные имена и соответствующие им I2P адреса. Из чего можно заключить, что вычислить пользователя по DNS запросам практически невозможно.

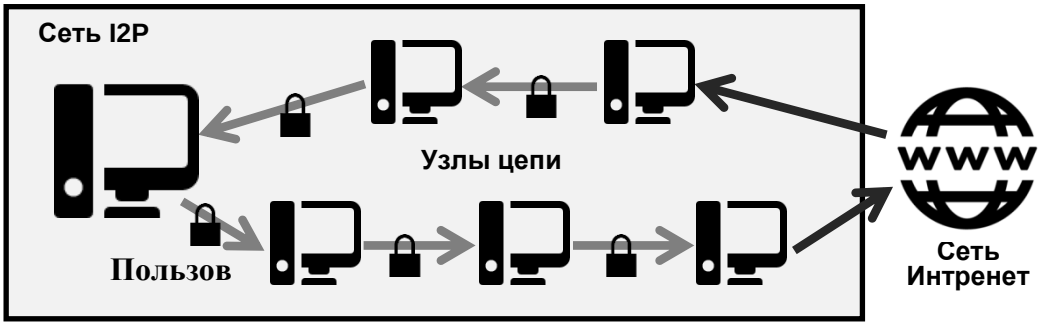


Рис. 4. Принципиальная схема построения маршрутов в сети I2P

Особенность сети I2P заключается в том, что она в основном используется, как полноценная и самостоятельная сеть, которая имеет свою адресацию и свои Web-сайты, называемые eepsites. В таком случае она действительно обеспечивает очень высокий уровень анонимизации. Если же её использовать для выхода в сеть Интернет, то возникает проблема безопасности, так как на выходном узле из сети I2P трафик может быть изменён или прослушан. Более того для пользователя предоставляется только один выходной узел, а это значит, что может возникнуть проблема с блокировкой на некоторых сайтах.

Метод «крышевания» доменов.

Методы и средства, обеспечивающие анонимность, постоянно развиваются. Сейчас активно набирает популярность описанный в 2015 году метод «крышевания доменов». В оригинальном источнике этот метод называется domain fronting. Рассмотрим его на примере известного мессенджера «Signal». Для обеспечения анонимности он использует широко признанное, авторитетное промежуточное звено между пользователем и Web-сервером. А именно службу хостинга сайтов «Google App Engine» [8]. На рис. 5. представлена принципиальная схема работы метода «крышевания» доменов. Особенность такого метода заключается в том, что средства, анализирующие трафик, воспринимают такие запросы, как обращение к различным доменам Google и рассматривают их в качестве конечного звена. На самом же деле реальное доменное имя зашифровано с помощью HTTPS шифрования и после прохождения промежуточного узла, трафик перенаправляется далее по необходимому адресу уже с IP адресом сервера Google. Для блокировки такого метода необходимо заблокировать все домены, которые предоставляет служба «Google App Engine», что является затруднительным.

Метод «крышевания доменов» зависит от промежуточного Web-сервера, а значит, вновь возникает проблема доверия. Недостаток рассмотренного мессенджера заключается в том, что к аккаунту привязывается номер мобильного телефона, а все контактные номера с устройства выгружаются на сервер, для того, чтобы организовать пересылку сообщений. Таким образом,

информация о пользователе, которую можно найти в сети Интернет, привязывается к информации, которая храниться на серверах мобильных операторов.

Рис. 5. Принципиальная схема работы метода «крышевания» доменов

Как видно, ни один из разобранных в статье способов не может дать гарантию полной анонимности. Всегда остаются уязвимости систем, которыми могут воспользоваться с целью деанонимизации [9]. Поэтому прежде, чем выбирать способ скрытия личности в сети, необходимо чётко определить с какой целью он будет использован и оценить на какие затраты средств и времени будут готовы пойти злоумышленники, чтобы провести деанонимизацию. К примеру, если главная задача — это не допустить утечку данных рекламным компаниям, то будет достаточно воспользоваться proxy-серверами и чистить файл cookies. При этом лучше избегать посещения социальных сетей. В условиях, когда провайдером блокируется часть Интернет ресурсов, особенно часто применяются средства анонимизации для получения доступа к запрещённым доменам. В таком случае помимо Proxy-серверов пользуются сетью Tor, поскольку она считается более надёжным методом достижения анонимности в сети. Если этот способ применяется с целью анонимного посещения Web-серверов сети Интернет, то, как правило, большинство атак будет сводиться к принципу «цель не оправдывает средства». Тем не менее, в настоящее время активно исследуются способы противодействия Tor. В качестве же системы для передачи личных данных лучше использовать I2P без выхода в сеть Интернет. Поскольку сеть I2P обеспечивает не только анонимность, но и безопасность передаваемых данных.

Заключение. В работе были рассмотрены подходы к обеспечению анонимности в сети. Ни один способ на сегодняшний день не может обеспечить полной анонимизации пользователя. Поэтому задача анонимизации сводится к тому, чтобы для деанонимизации требовались недостижимые вычислительные ресурсы или такой объем времени раскрытия, что по его истечению деанонимизация была бы уже не актуальной. Также при использовании различных методов возникают сопутствующие трудности. Поэтому, выбирая средства, следует учитывать, какой ценой будет обеспечиваться анонимность. Для того чтобы избавиться от некоторых недостатков того или иного метода анонимизации прибегают к комбинированию различных методов. Как показывает практика, на каждый метод анонимизации создаются средства, позволяющие обойти его. Поэтому, вероятнее всего, «панацеи» в средствах обеспечения анонимизации создано не будет. Со стороны нашего государства отношения в сфере информационной безопасности регулируются 23 и 24 статьей Конституции РФ. Каждый имеет право на неприкосновенность частной жизни, однако реализация этого права в руках каждого участника информационного обмена. Знание элементарных основ информационной безопасности решит большую часть проблем обеспечения анонимности.

СПИСОК ЛИТЕРАТУРЫ

1. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. – 4-е изд. – М., 1997.
2. Steel. E., Jessica E. Vascellaro. Facebook, MySpace Confront Privacy Loophole // www.wsj.com, 21.05.2010. Точныйадресстатьи: http://www.wsj.com/articles/SB10001424052748704513104575256701215465596.
3. Радайкин М.Ф. Кратко о проблеме анонимности в сети интернет // Пробелы в российском законодательстве. Юридический журнал. 2013. №2 С. 25-28.
4. Денисова Т.Б. Безопасность услуги VPN//Вестник Самарского государственного технического университета. Серия: технические науки. 2005. №33 С. 168-171.
5. Иванов С.Н. Преступление в сфере высоких технологий: проблемы документирования компьютерных преступлений// Юридическаянаука и практика: Вестник Нижегородской академии МВД России. 2012. № 18 С. 70-74.
6. Кузичкина О.А. Сеть Tor как способ подключения к «глубокому» интернету // Интеллектуальный потенциал XXI века: ступени познания. 2014. №25 С. 129-131.
7. Угрюмов Д.В., Хализев В.Н. Создание математической модели обеспечения достаточного уровня анонимности в системах электронного голосования с сохранением целостности и конфиденциальности передаваемых данных // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2013. №93 С. 1-16.
8. Fifield D., Lan C., Hynes R., Wegmann P., Paxon V. Blocking-resistant communication through domain fronting // Proceedings on Privacy Enhancing Technologies. 2015. N 2. P. 1-19.
9. Ахметшин Р.Г., Киселева Л.В. анонимность в глобальной сети // Вестник молодых ученых Самарского государственного экономического университета. 2016. № 1 (33). С. 265-269.

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА: БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.85

ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ В ГЛУБОКОМ АНАЛИЗЕ СЕТЕВОГО ТРАФИКА

Безверхняя Екатерина Александровна
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mail: kate.bezverkhnyaya@gmail.com

Аннотация. В докладе рассмотрены пять алгоритмов машинного обучения, с помощью которых осуществляется фильтрация шифрованного сетевого трафика отдельно взятой подсети: NaıveBayes, NBTree, LibSVM, J4.8, AdaBoost+J4.8. В результате сравнения скорости работы и необходимого количества пакетов потока для определения соответствия между потоком трафика и веб-службой для каждого из алгоритмов, определены два самых эффективных.

Ключевые слова: *машинное обучение; анализ сетевого трафика; классификация; сетевое администрирование.*

APPLICATION OF MACHINE LEARNING IN DEEP TRAFFIC ANALYSIS

Alexandrovna Ekaterina
St. Petersburg National Research University information technology, mechanics and optics,
Russia, St. Petersburg, Kronverkskiy pr.,49
e-mail: kate.bezverkhnyaya@gmail.com

Abstract. The report describes five machine learning algorithms, which are used to filter the encrypted network traffic of a single subnet: NaıveBayes, NBTree, LibSVM, J4.8, AdaBoost+J4.8. Two of the most efficient algorithms are identified by comparing the speed and number of flow packets required to determine the correspondence between the traffic flow and the web service for each algorithm.

Keywords: *machine learning; analysis of network traffic; classification; network administration.*

Сетевой анализ является полезным и иногда важным инструментом в области сетевого администрирования. Он используется провайдерами интернет-услуг (Internet Service Providers - ISP) для мониторинга трафика в своих сетях и обеспечения постоянного качества обслуживания (Quality of Service - QoS) для своих клиентов [3]. Сетевые администраторы могут использовать инструменты сетевого анализа, которые обнаруживают вторжение вредоносных программ и обеспечивают фильтрацию данных, что позволяет автоматически блокировать и сообщать о подобных сообщениях [2]. Однако шифрование служит препятствием для анализа таких сообщений [2]. Многие традиционные устройства сетевого анализа не могут эффективно анализировать зашифрованный сетевой трафик. Все больше приложений перемещается в облако и использует веб-сервисы [6, 7]. Эти веб-службы часто используют шифрование сетевых протоколов, таких как Transport Layer Security (TLS) [5, 9, 10]. По мере увеличения количества TLS трафика, возможность изучения потоков TLS для анализа рисков безопасности становится более важной.

Это исследование предоставляет способ быстрой классификации веб-службы в рамках зашифрованного сетевого трафика, построенный на основе анализа способности алгоритмов машинного обучения (Machine Learning - ML) классифицировать приложения и протоколы, оперируя их сетевым трафиком [8]: Naıve Bayes, NBTree, LibSVM, J4.8, AdaBoost+J4.8/ Дальнейшие исследования показывают возможность использования алгоритмов ML для определения того, связано ли приложение с зашифрованным потоком [1]. ML-алгоритмы также полезны при классификации сетевого трафика в режиме реального времени [4]. Измеряя эффективность алгоритмов ML при классификации 16 типов веб-сервисов в потоках TLS. Предполагается, что проверенные алгоритмы ML смогут успешно классифицировать веб-службы, связанные с зашифрованными сетевыми потоками. Кроме того, предполагается, что точность и время выполнения алгоритмов ML будут увеличиваться по мере увеличения количества анализируемого сетевого трафика. Целью этого исследования является повышение способности устройств сетевого анализа уменьшать вторжение вредоносных программ и фильтрацию данных через зашифрованные сетевые

коммуникации. Хотя метод, проанализированный в этом исследовании, не пытается идентифицировать конкретные случаи вторжения или провести фильтрацию, он позволяет применять более широкие политики для смягчения этих рисков. Классифицируя зашифрованные веб-службы, сетевые администраторы могут обнаруживать и предотвращать использование несанкционированных веб-сервисов. Для достижения поставленной цели, нужно решить две задачи: - оценить, какие алгоритмы ML, вероятно, будут хорошо выполняться при классификации зашифрованного веб-трафика. Начальные эксперименты выполняются для проверки каждого из пяти алгоритмов ML над идентичным набором трафика. Алгоритмы, которые работают лучше всего с точки зрения точности и времени выполнения, используются для оставшейся части экспериментов. Вторая цель этого исследования - определить, сколько пакетов необходимо для достижения приемлемой точности классификации. Предполагается, что время выполнения и точность будут увеличиваться по мере увеличения количества анализируемых пакетов. Хотя решение, которое оптимизирует обе метрики, вероятно, не существует, это исследование количественно оценивает каждую метрику индивидуально для увеличения анализируемых потоков, начиная с начала потока.

В этом исследовании представлены два алгоритма ML для использования при классификации веб-службы в зашифрованном потоке TLS и показывает, что алгоритмы ML могут достичь в этом контексте приемлемой точности. По мере того, как все больше приложений переходит на веб-услуги или облачные сервисы, это становится все более важным. В дополнение к внедрению способности алгоритмов ML классифицировать веб-сервисы, это исследование также расширяет число меток, используемых в исследованиях классификации трафика на основе ML. Он также непосредственно анализирует эффективность использования AdaBoost в сочетании с J4.8 в классификации веб-сервисов. Также анализируется время, необходимое для классификации зашифрованного потока трафика на современных системах. Используемый набор функций с выбранными двумя алгоритмами показывает отличные результаты возможностью алгоритма ML классифицировать недельный трафик уровня TLS менее чем за 5 секунд, используя медленные алгоритмов. Эта скорость классификации показывает возможность использования этого метода для предотвращения вторжений вредоносных программ и предотвращения фильтрации данных в устройствах анализа сети в режиме реального времени.

СПИСОК ЛИТЕРАТУРЫ

1 Альшаммари, Р. и А. Н. Цинсир-Хейвуд. «Обобщение подписей для идентификации шифрованного трафика SSH». Вычислительный интеллект в кибербезопасности, 2009. CICS '09. Симпозиум IEEE, 167-174. 2009.
2 Бордерс, К. и А. Пракаш. «Количественное определение утечек информации в исходящей веб-трафике». Безопасность и конфиденциальность, 2009 г. 30-й симпозиум IEEE, 129-140. 2009. ISBN 1081-6011.
3 Браун, Л., Г. Мунз и Г. Карл. «Пакетная выборка для обнаружения червя и ботнета в TCP-соединениях». Симпозиум по сетевым операциям и управлению (NOMS), 2010 IEEE, 264-271. ISBN 1542-1201.
4 Канини, Марко, Вэй Ли, Мартин Задник и Эндрю У. Мур. «Опыт высокоскоростной автоматической идентификации приложений для управления сетью». Материалы 5-го симпозиума ACM / IEEE по архитектуре сетей и систем связи, ANCS '09, 209-218. ACM, Нью-Йорк, Нью-Йорк, США, 2009. ISBN 978-1-60558-630-4. URL http://doi.acm.org/10.1145/1882486.1882539.
5 Констин, Джош. «Facebook может замедлить крошечный бит, когда он начнет переключать всех пользователей на безопасные HTTPS-соединения», 8 ноября 2012 года.
6 Кусумано, Майкл. «Облачные вычисления и SaaS - новые вычислительные платформы». Сообщения ACM, 53 (4): 27-29, 2010.
7 Кэмпбелл-Келли, Мартин. «Исторические размышления: подъем, падение и воскрешение программного обеспечения как службы». Сообщения ACM, 52 (5): 28-30, 05 2009. URLhttp://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=39363001&site=ehost-live.
8 Мур, Эндрю У., Денис Зуев и Майкл Кроган. Дискриминаторы для использования в классификации, основанной на потоках. Технический отчет RR-05-13, факультет компьютерных наук, Королева Мэри, Лондонский университет, август 2005 года.
9 Райт, Чарльз В., Фабиан Монроуз и Джеральд М. Массон. Msgstr "Выполнение поведения протокола приложения в зашифрованном сетевом трафике". Журнал исследований машинного обучения, 7 (12): 2745-2769, 12 2006. URLhttp://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=23757985&site=ehost-live.
10 Салливан, Дэнни. «Google начнет шифрование поисков и исходящих кликов по умолчанию с помощью SSL-поиска», 18 октября 2011 г. 2011 г.

УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

Бондарева Анастасия Дмитриевна, Гоман Елена Вячеславовна
Университет ИТМО
Россия, Санкт-Петербург, Кронверский пр., 49
e-mails: Bondareva.AD@yandex.ru, nen7995ka@mail.ru

Аннотация. Предложено определение автоматизированной системы управления технологическим процессом. Определено, что АСУ ТП является объектом информатизации, реализующим информационную технологию с использованием технических средств и систем. Предложен системный подход к обеспечению информационной безопасности АСУ ТП.

Ключевые слова: *автоматизированные системы управления технологическим процессом; объект информатизации; системный подход; информационная безопасность.*

ENSURING INFORMATION SAFETY OF AUTOMATED SYSTEMS OF TECHNOLOGICAL PROCESS CONTROL

Bondareva Anastasia, Goman Elena
ITMO University, Russia, St. Petersburg, Kronverksky pr., 49
e-mails: Bondareva.AD@yandex.ru, nen7995ka@mail.ru

Abstract. This article proposes the definition of an automated process control system. It is determined that automated process control system is an informatization object, realizing information technology with the use of technical means and systems. A system approach to ensuring information security of the automated process control system is proposed.

Keywords: *automated process control system; informatization object; system approach; information security.*

В настоящее время на предприятиях повсеместно используются автоматизированные системы управления технологическим процессом (АСУ ТП). Они предназначены для повышения эффективности производственного процесса, повышения безопасности в аварийных ситуациях и уменьшения затрат на производство.

Недостаточное понимание, что представляет собой данная система, какая информация подлежит защите и каким способом осуществлять ее защиту, создает проблематику обеспечения информационной безопасности АСУ ТП. В целях повышения эффективности обеспечения ИБ предприятий очевидна постановка задачи о разработке единого обобщенного подхода к обеспечению защиты информации (ЗИ) на АСУ ТП.

Для решения поставленной задачи было проведено исследование законодательной и нормативно-правовой базы РФ в области информационной безопасности, в процессе которого было выявлено, что отсутствует четкое и понятное определение АСУ ТП. Принимая во внимание определения «автоматизированная система» [1] и «технологический процесс» [2] представляется целесообразным сформулировать понятие АСУ ТП как «система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию управления частью производственного процесса, содержащей целенаправленные действия по изменению и (или) определению состояния предмета труда».

Так как в любой автоматизированной системе хранится и обрабатывается информация, то от защищенности данной информации зависит корректность и непрерывность функционирования АС, а соответственно и защищенность интересов организации.

При обеспечении информационной безопасности (ИБ) организации основополагающим понятием является «объект защиты информации». Исходя из [3] в автоматизированной системе управления объектами защиты является не только информация о параметрах управляемого объекта или процесса, но и программно-технический комплекс, включающий технические средства, программное обеспечение (ПО), а также средства защиты информации (СрЗИ). Это означает, что при обеспечении ИБ организации, использующей АСУ ТП, следует говорить не о самой АС, а об объекте АСУ ТП.

Таким образом, с одной стороны объектом защиты информации на предприятии будет являться объект АСУ ТП, включающий в себя защищаемую информацию и комплекс средств автоматизации, обеспечивающий технологию ее обработки. С другой стороны, в качестве «Объектов защиты информации» в соответствии с моделью объекта защиты информации [4] определены объекты информатизации предприятия (ОИ). ОИ подразделяются на объекты информатизации, реализующие ИТ с использованием технических средств и систем (ОИ_ТСС) и объекты информатизации, предназначенные для ведения конфиденциальных переговоров. Таким образом, если при обработке информации используются технические средства, то следует говорить о первом типе объекта информатизации.

При соотнесении структуры понятий объекта АСУ ТП и ОИ_ТСС, было выявлено, что понятие ОИ_ТСС шире и включает в себя объект АСУ ТП. Это позволяет сделать вывод, о том, что объект АСУ ТП является объектом информатизации, реализующим информационную технологию с использованием технических средств и систем.

Анализ законодательной и нормативно-правовой базы РФ в области информационной безопасности показал, что нет ни одного конкретного решения по обеспечению ИБ АСУ ТП кроме приказа ФСТЭК №31, который предназначен для обеспечения ЗИ в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Это означает, что защита информации на объектах АСУ ТП предприятий, не связанных с вышеперечисленными областями, не регулируется данным приказом и может быть обеспечена мерами защиты, в нем не описанными. С другой стороны,

приказ содержит точные и понятные инструкции по защите АСУ ТП и не запрещает их использование на других объектах.

Так как объект АСУ ТП является ОИ_ТСС, то представляется возможным обеспечивать его информационную безопасность на основе системного подхода, являющегося обобщенным для всех ОИ и не противоречащим требованиям Приказа ФСТЭК №31. В качестве используемого в системном подходе методологического средства предлагается использование моделирования различных этапов разработки подсистемы технической защиты информации.

Важно помнить, что организация и функционирование СЗИ должны осуществляться в соответствии с циклической моделью Дёминга и информационная безопасность ОИ должна обеспечиваться на всех этапах его жизненного цикла.

Заключение:

1. Предложено определение автоматизированной системы управления технологическим процессом.

2. Определен объект АСУ ТП как объект информатизации, реализующий информационную технологию с использованием технических средств и систем.

3. Предложен системный подход к обеспечению безопасности ИБ АСУ ТП являющийся универсальным и не противоречащим приказу ФСТЭК №31.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения // Каталог национальных стандартов – Росстандарт. 2017. URL: http://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=129578 (дата обращения 12.09.2017)
2. ГОСТ 3.1109-82 “Единая система технологической документации. Термины и определения основных понятий”URL: http://gostexpert.ru/gost/gost-3.1109-82 (дата обращения 12.09.2017)
3. Приказ ФСТЭК от «14» марта 2014 г. №31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» URL: http://fstec.ru/rss-lenta/110-tekhnicheskaya-zashchita-informatsii/dokumenty/prikazy/864-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения 15.09.2017)
4. Загородников А.А., Козлов С.В. Модель объекта защиты информации // Конференция участников ГПО ТУСУР 2014. URL: https://gpo-conference.tusur.ru/conference/2014/themes/99/projects/571/discourses/654 (дата обращения 16.09.2017)

УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАЩИЩЕННОСТИ ОСУЩЕСТВЛЕНИЯ ФИНАНСОВЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЕСКОНТАКТНОЙ ОПЛАТЫ

Ганчикова Юлия Сергеевна, Курышева Алена Андреевна
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр.,49
e-mails: yul7494582@yandex.ru, kurysheva.al@yandex.ru

Аннотация. Проводится анализ защищенности операций с использованием технологий бесконтактных платежей. Рассмотрены принципы работы технологий и обеспечения безопасности бесконтактных расчетов.

Ключевые слова: *финансовая безопасность; бесконтактные платежи; NFC; транзакции; защита.*

COMPARATIVE ANALYSIS OF FINANCIAL TRANSACTIONS SECURITY USING CONTACTLESS PAYMENT TECHNOLOGIES

Ganchikova Yulia, Kurysheva Alena
St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverksky pr.,49
e-mails:yul7494582@yandex.ru, kurysheva.al@yandex.ru

Abstract. The analysis of security transactions using contactless payment technologies is carried out. The paper considered the principles of work of technologies and provision of security of contactless calculations.

Keywords: *financial security; contactless payments; NFC; transaction; security.*

В настоящее время технологии бесконтактной оплаты используются всё более широко. В связи с этим вопрос защищенности бесконтактных технологий является крайне актуальным. От уровня защищенности напрямую зависит сохранность денежных средств и персональных данных.

Бесконтактная оплата может быть произведена с помощью карты или с помощью смартфона. Для сравнения технологий бесконтактной оплаты были использованы «MasterCard PayPass», «Apple Pay», «Samsung Pay» и «Android Pay». Технологии сравнивались по стандартам, идентификации, аутентификации, инструментам и дополнительной защите. Сравнительный анализ показал, что в

первую очередь различаются данные необходимые для аутентификации и идентификации пользователя.

На основе сравнительного анализа можно сделать вывод, что каждая из рассмотренных технологий и систем проведения платежа имеет ряд особенностей. Введение дополнительного уровня безопасности обеспечивает более эффективную защиту транзакций. Для повышения уровня защищенности технологий бесконтактной оплаты и надежности хранения персональных данных следует уделить особое внимание использованию дополнительных системы защиты и повышенному уровню аутентификации.

СПИСОК ЛИТЕРАТУРЫ

1. Никонец О. Е., Гринь И. А., Марченко А. В. Бесконтактные платежи: история возникновения и безопасность // Научно-методический электронный журнал «Концепт». – 2016. – Т. 15. – С. 2726–2730. – URL: http://e-koncept.ru/2016/96466.htm (дата обращения: 16.09.2017).
2. О мерах безопасного использования банковских карт [Электронный ресурс] : Письмо ЦБР от 2 октября 2009 г. №120-Т. Доступ из справ.-правовой системы «Гарант».
3. О национальной платежной системе [Электронный ресурс] : федер. закон Рос. Федерации от 27 июня 2011 г. №161-ФЗ : принят Гос. Думой 14 июня 2011 г. : одобр. Советом Федерации 22 июня 2011 г. (ред. от 18.07.2017). Доступ из справ.-правовой системы «КонсультантПлюс».

УДК 005.922.1

ОБЗОР DLPСИСТЕМ

Герцен Дмитрий Михайлович, Стафеев Алексей Владимирович, Сердюков Никита Васильевич
Санкт-Петербургский государственный аэрокосмического приборостроения
Россия, Санкт-Петербург, ул. Большая морская, 67
e-mails: sierra@live-cs.ru, alekseystafeev@gmail.com, uthw@yandex.ru

Анотация.В статье рассмотрены DLP системы InfoWatch TrafficMonitor, FalconGaze SecureTower, Digital Guardian (Verdasys).

Ключевые слова: *DLP; InfoWatch; FalconGaze; Digital Guardian; сравнение систем; информационная безопасность.*

OVERVIEWODLPSYSTEMS

Gerzen Dmitry, Stafeev Aleksey, Serdyukov Nikita
St. Petersburg State University of Aerospace Instrumentation
Russia, St. Petersburg, Bolshaya Morskaia str., 67
e-mails: sierra@live-cs.ru, alekseystafeev@gmail.com, uthw@yandex.ru

Abstract. The article presents DLP systems InfoWatch TrafficMonitor, FalconGaze SecureTower, Digital Guardian (Verdasys).

Keywords: *DLP; InfoWatch; FalconGaze; Digital Guardian; comparison of systems; information security.*

Введение. Системы защиты от утечек конфиденциальной информации (Data Loss Prevention - DLP) предназначены для отслеживания и блокирования попыток несанкционированной передачи данных за пределы корпоративной сети. Помимо предотвращения утечек информации Современные DLP-системы помимо основных вмещают в себя также функции обнаружения информации (eDiscovery), шифрования (Encryption), а также контроля действий персонала и повышения его производительности (Employee Management Software и Productivity Control).

Использование DLP системы наиболее актуально для организаций, где риск утечки конфиденциальной информации повлечет серьезный финансовый или репутационный ущерб, а также для организаций, которые настороженно относятся к лояльности своих сотрудников. Решения класса DLP по предотвращению утечек информации обеспечивают защиту такой конфиденциальной информации, как условия тендеров, заказы на услуги и решения, номера пластиковых карт, сведения о счетах клиентов, персональные данные сотрудников и клиентов, финансовые данные и т.д.

Основными каналами утечки информации являются:

– съемные носители: USB – флеш – накопители, CD/DVD диски, съемные, жесткие диски и пр.;
– электронная почта, в том числе личная;
– распечатанные с компьютера документы;
– социальные сети, Skype, ICQ и пр.

Основные функции DLP систем:

– контроль передачи информации через Интернет с использованием E-Mail, HTTP, HTTPS, FTP, Skype, ICQ и других приложений и протоколов;
– контроль сохранения информации на внешние носители - CD, DVD, flash, мобильные телефоны
– защита информации от утечки путем контроля вывода данных на печать;

– блокирование попыток пересылки/сохранения конфиденциальных данных, информирование администраторов ИБ об инцидентах, создание теневых копий, использование карантинной папки;

– поиск конфиденциальной информации на рабочих станциях и файловых серверахпо ключевым словам, меткам документов, атрибутам файлов и цифровым отпечаткам;

– предотвращение утечек информации путем контроля жизненного цикла и движения конфиденциальных сведений.

Обычно система класса DLP включает следующие компоненты:

– центр управления и мониторинга;

– агенты на рабочих станциях пользователей;

– сетевой шлюз DLP, устанавливаемый на Интернет-периметр.

DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

Распознавание конфиденциальной информации в DLP-системах производится двумя способами:

– Анализ формальных признаков

(например, грифа документа, специально введённых меток, сравнением хэш-функции)

позволяет избежать ложных срабатываний (ошибок первого рода), но зато требует предварительной классификации документов, внедрения меток, сбора сигнатур и т.д. Пропуски конфиденциальной информации (ошибки второго рода) при этом методе вполне вероятны, если конфиденциальный документ не подвергся предварительной классификации.

– Анализом контента

Даёт ложные срабатывания, зато позволяет выявить пересылку конфиденциальной информации не только среди грифованных документов. В хороших DLP-системах оба способа сочетаются.

В состав DLP-систем входят компоненты (модули) сетевого уровня и компоненты уровня хоста.

Сетевые компоненты контролируют трафик, пересекающий границы информационной системы. Обычно они стоят на прокси-серверах, серверах электронной почты, а также в виде отдельных серверов. Компоненты уровня хоста стоят обычно на персональных компьютерах работников и контролируют такие каналы, как запись информации на компакт-диски, флэш-накопители и т.п.

Хостовые компоненты также стараются отслеживать изменение сетевых настроек, инсталляцию программ для туннелирования, стеганографии и другие возможные методы для обхода контроля. DLP-система должна иметь компоненты обоих указанных типов плюс модуль для централизованного управления.

Рассмотрим и сравним несколько DLP систем:

1) InfoWatchTrafficMonitor.

Архитектура (Рисунок 1):

– InfoWatch Traffic Monitor — модуль для контроля сетевых каналов передачи данных. Передача информации через сетевые каналы передачи данных (web-сервисы, почтовые и файловые сервера, сервисы мгновенных сообщений) осуществляется через сетевой шлюз, который также передает перехваченные данные на сервер Traffic Monitor.

– InfoWatch Device Monitor — модуль для защиты рабочих станций, осуществляющий контроль печати и копирования документов на съемные носители, а также контроль портов и съемных устройств.

– InfoWatch Crawler — модуль для контроля информации в общедоступных сетевых хранилищах и системах документооборота, осуществляет сканирование и применение политик к информации, хранящейся «в покое», а также поддерживает в актуальном состоянии эталонные документы и выгрузки.

– InfoWatch Forensic Storage — специализированное хранилище, содержащее архив всех информационных потоков организации, в том числе нарушения политик безопасности и факты утечек конфиденциальной информации.

– InfoWatch Device Monitor Mobile – модуль контроля мобильных устройств. Модуль контролирует работу сотрудников с электронной почтой, веб-ресурсами, фотографиями и сервисами обмена сообщениями на мобильных устройствах.

– InfoWatch Vision – модуль визуальной аналитики информационных потоков в режиме реального времени.

InfoWatch предоставляет несколько вариантов для среднего (Standard Solution) и крупного бизнеса (Enterprise).

2) Falcongaze SecureTower

– Сервис централизованного перехвата – компонент, который представляет собой шлюзовое решение и отвечает за получение и начальную обработку трафика. Это позволяет контролировать весь трафик, покидающий периметр сети.

– Список контролируемых протоколов: POP3, SMTP, IMAP, OSCAR (ICQ и тд), XMPP, HTTP, FTP, MRA, YIM, MAPI.

– Сервис событий и уведомлений – фиксирует все события в работе сервиса централизованного перехвата и при необходимости отправляет уведомления администратору системы, если произошло важное событие или сбой.

– Сервис контроля агентов – применяется для работы с агентами, которые инсталлируются на рабочие станции сотрудников. Позволяет перехватывать информацию, передаваемую по шифрованным каналам (Skype, SSL).

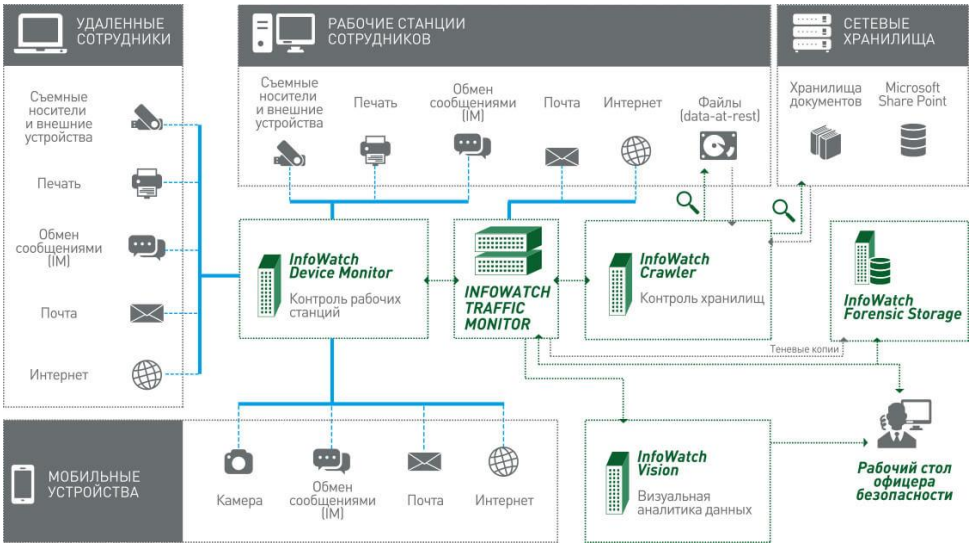


Рисунок 5. Модель Архитектуры InfoWatchTrafficMonitor

Также в агентах реализован функционал блокировки нежелательной информации по протоколам SMTP, HTTP, HTTPS.

– Сервис обработки почты – компонент для перехвата почтовых сообщений, которые проходят через корпоративный почтовый сервер.

– Сервер ICAP – получает HTTP/HTTPS трафик от прокси-серверов с поддержкой протокола ICAP.

– Сервис обработки данных – данный компонент необходим для решения целого ряда задач: лицензирования для других компонентов SecureTower, индексирования перехваченных данных, работы с цифровыми отпечатками документов, осуществления операций поиска и прочее.

– Сервис распознавания изображений – предназначен для распознавания текстовой информации на пересылаемых изображениях.

– Сервис обеспечения безопасности и отчетов – отвечает за построение разнообразных отчетов и работу правил безопасности.

– Сервис идентификации пользователей – компонент, позволяющий администраторам управлять данными о контролируемых пользователях, а также обеспечивающий аутентификацию в SecureTower.

– Перехват трафика с возможностью его блокировки - SecureTower 5.5 позволяет не только перехватывать трафик, но и блокировать его.

– Контроль локальных каналов утечки информации - реализован инструментарий для контроля устройств, подключенных к компьютеру по внутренним интерфейсам.

– Контроль печати документов.

– Распознавание форматов файлов.

– Технологии контентного анализа.

– Отслеживание активности пользователей на рабочих станциях.

– Система отчетности - отличается большим количеством статистических отчетов, которые позволяют получить полную картину сетевой активности сотрудников.

– Граф-анализатор взаимосвязей персонала.

– Права доступа - реализована гибкая система разграничения прав доступа к компонентам.

– Защита агентов - защита от завершения работы процесса агента или его удаления, а также предусмотрена возможность скрытой работы, при которой присутствие агента на компьютере становится незаметным для пользователя.

3) Digital Guardian (Verdasys):

DigitalGuardian состоит из четырех модулей:

– Network DLP - представляет собой аппаратное решение либо ПО, которое устанавливается в точках сети. Она анализирует сетевой трафик для обнаружения конфиденциальных данных;

– DLP Discover – находит ваши конфиденциальные данные, даже если их местоположение неизвестно.

– Endpoint DLP – обеспечивает защиту данных от утечек через настольные и портативные пользовательские компьютеры, находящиеся как в корпоративной сети, так и вне ее. Cloud DLP - позволяет компании использовать облачное хранилище с соблюдением правил конфиденциальности и защиты данных.

Архитектура

– Консоль управления - веб центр. Консоль позволяет создавать политики и отчеты, управлять ими.

– Агент - обеспечивает контроль над событиями системы отдельных пользователей. Вшит в ядро, контролирует процессы, события и данные из ОС. Агенты работают автономно, с полными знаниями всех систем, служб и исполняемых файлов, не полагаясь на подключение к консоли.

– Приборы мониторинга и управления сетью - Предотвращают утечку конфиденциальных данных организации. Контролируют весь сетевой трафик и обеспечивают соблюдение политик для обеспечения защиты.

Контролируемые сетевые каналы: HTTP/HTTPS, FTP, P2P, SSL, E-mail (SMTP), Office365

Контролируемые локальные каналы: USB, Wi-Fi, Bluetooth, Локальные принтеры, CD/DVD, PrintScreen, Encrypt/Compress.

Контролируемые базы данных: MSSQL, Oracle, MySQL, DB2, Sybase, Informix, PostgreSQL.

Контролируемые облачные хранилища: Box, O365 (OneDrive), Egnyte, CitrixFileshare, Accellion.

– Технологии распознавания информации.

Цифровые отпечатки – сравнение перехваченной информации с образцами конфиденциальных документов. Распознает конфиденциальный документ после частичного удаления, копирования и перемещения данных внутри документа, копирования данных в другой документ, маскировки отдельных символов, изменения формата или кодировки документа и т.д.

Сигнатуры – целочисленные константы, используемые для однозначной идентификации ресурса или данных. Регулярные выражения – формальный язык поиска и осуществления манипуляций с подстроками в тексте, основанный на использовании метасимволов.

Механизмы извлечения текста из изображений – некоторые файлы JPEG имеют верхние и нижние колонтитулы и другие фрагменты контента, где можно извлечь текст и проверить его.

Теневое копирование – при записи файлов на внешний носитель копия записываемых данных вместе с дополнительной информацией (имя пользователя, приложение, дата, время) сохраняется на жестком диске компьютера и в дальнейшем переносится на сервер.

Возможности для проактивного предотвращения утечек (аналитика)

– Сканирование хранилищ данных в режиме реального времени;

– Предоставляет информацию о всей системе Digital Guardian, включая устройства, состояние работоспособности, события, уведомления о отчетах, запланированные задания и очереди.

– Оповещения. Показывает общее количество предупреждений, генерируемых правилом или политикой за определенный период.

– События. Отображает обзор общих событий данных, включая общую активность и активность конкретного пользователя.

– Инвентаризация файлов - отчеты о данных в состоянии покоя; инвентаризация всех секретных файлов на конкретном компьютере.

– Обнаружение файлов. Предоставляет информацию о нарушениях политики обнаружения.

– Электронная почта. Отображает обзор всей активности электронной почты на предприятии.

– Нарушение правил пользователем. Определяет тенденции для отдельных пользователей или компьютеров.

Сравнение DLP систем:

Таблица 1

Достоинства DLP систем

InfoWatch Traffic Monitor	Digital Guardian (Verdasys)	Falcongaze SecureTower
Полный контроль над конфиденциальным оборотом данных	Клиенты сообщают о быстром развертывании и успешных проектах при использовании продукта Digital Guardian в сочетании с их службами управления.	Данный продукт прост в развертывании и эксплуатации, благодаря чему с успехом может использоваться не только в средних и крупных, но и в небольших компаниях.
Соблюдение внутренних политик и стандартов, внешних правил и положений, отраслевых стандартов (например, PCI DSS, SOX,	Digital Guardian интегрируется с более широкими продуктами безопасности, включая информацию об угрозах, сетевую песочницу, поведенческий анализ (UEBA), защиту облачных	эффективные инструменты для анализа сетевой активности персонала и контроля рабочего времени.

GLBA, HIPAA) и требований безопасности клиентов	данных, информацию о безопасности и управление событиями (SIEM, включая приложения, доступные в магазинах приложений IBM QRadar и Splunk).	
Смягчение финансовых, юридических и репутационных рисков, связанных с потерей данных	Клиенты, такие как модульное лицензирование для Endpoint DLP, поддерживают Windows, Mac OS X и Linux, а также возможности конечных точек, которые могут быть лицензированы в любой комбинации видимости и управления устройства, DLP и расширенной защиты от угроз.	---
Улучшение корпоративной культуры путем обучения сотрудников в отношении реализации политики безопасности	Digital Guardian демонстрирует хорошее понимание технологий, безопасности, возможных угроз и тенденций в отрасли.	---

Таблица 2

Недостатки DLP систем

InfoWatch Traffic Monitor	Digital Guardian (Verdasys)	Falcongaze SecureTower
Веб-консоль InfoWatch Traffic Monitor поддерживает работу только с Google Chrome.	отсутствует общая политика в отношении конечных точек и сетевых продуктов.	отсутствие возможности поиска конфиденциальных данных на рабочих станциях в корпоративной сети, однако в планах у разработчиков данного решения стоит реализация данной функции в ближайшем будущем
Нет контроля поисковых запросов пользователей	Агент Digital Guardian не может различать личные и корпоративные учетные записи Microsoft OneDrive. Это может помешать использованию личного приложения Microsoft OneDrive.	не имеет в своем арсенале некоторых перспективных методов анализа перехватываемого контента, например, технологий искусственного интеллекта (построенных на машинном обучении), контроля движения отсканированных документов, документов с печатями, цифровых отпечатков для бинарных документов.
Нет перехвата протоколов YMSG, MSN, P2P	Клиенты выразили озабоченность по поводу скорости интеграции CGN (Code Green Networks).	отсутствие встроенного категоризатора веб-сайтов
Нет контроля IP-телефонии	Фильтрация структурированных данных не поддерживается агентом конечной точки Digital Guardian, но эта функция доступна через агента CGN.	слабую интеграцию со сторонними продуктами.

СПИСОК ЛИТЕРАТУРЫ:

1. Официальный сайт DigitalGuardian. [Электронный ресурс], URL: https://digitalguardian.com (дата обращения: 15.09.2017)
2. Официальный сайт FalconGaze. [Электронный ресурс], URL: https://falcongaze.ru (дата обращения: 15.09.2017)
3. Официальный сайт InfoWatch. [Электронный ресурс], URL: https://www.infowatch.ru (дата обращения: 15.09.2017)

УДК 004.056

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ОДНОРАЗОВОГО БЛОКНОТА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ ПОТОКОВ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

Грозов Владимир Андреевич
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр.,49
e-mail: vladimirgrozov@mail.ru

Аннотация. В докладе рассмотрены особенности и возможности использования шифрования методом одноразового блокнота применительно к защите информационных потоков, возникающих в процессе эксплуатации беспилотного летательного аппарата. Обсуждаются риски, возможные при использовании широко распространенных алгоритмов шифрования. Приведены перспективные направления развития схемы одноразового блокнота.

Ключевые слова: *беспилотный летательный аппарат; одноразовый блокнот; псевдослучайная последовательность; шифрование.*

PROSPECTS OF ONE-TIME PAD USAGE FOR PROTECTION OFUNMANNED AERIAL VEHICLE DATASTREAMS

Grozov Vladimir
ITMO University
Russia, St. Petersburg, Kronverksky pr.,49
e-mail: vladimirgrozov@mail.ru

Abstract. The report presents the features and capabilities of the encryption method based on one-time pads for protection of information flows that occur in the process of operation of unmanned aerial vehicle. The risks that are possible when using common cryptographic algorithms are discussed. The promising directions of a one-time pad scheme development are represented.

Keywords: *one-time pad; unmanned aerial vehicle; pseudorandom sequence; encryption.*

Защита информационных потоков, возникающих при эксплуатации беспилотного летательного аппарата (БЛА), является сегодня очень актуальной задачей, поскольку несанкционированное вмешательство в его систему управления может привести к серьезному ущербу, вплоть до потери аппарата. Особенностями БЛА является передача по слабо защищенному от перехвата радиоканалу, а также ограниченные вычислительные ресурсы.

Ценность любой содержательной информации в современных условиях очевидна, и так же очевидны все возрастающие усилия заинтересованных сторон, направленные на завладение ею. Риск несанкционированного доступа усугубляется серьезной поддержкой нелегального сбора информации со стороны определенных структур, в том числе и государственных. На разработчиков программного обеспечения и соответствующего оборудования оказывают давление с тем, чтобы уже на этапе разработки предусматривались уязвимости в программных продуктах и устройствах [1]. В результате многие широко распространенные алгоритмы шифрования уже скомпрометированы, и, вполне возможно, что и остальные шифры ждет та же участь. Кроме того, приближается эра квантовых компьютеров, имеющих несопоставимо более высокую, по сравнению с обычными, скорость обработки данных. Это может сделать уязвимыми классические алгоритмы шифрования, построенные на принципе невозможности дешифрования за приемлемое время. В настоящее время стоимость действующих моделей квантовых компьютеров крайне высока из-за технических трудностей при обеспечении их нормальной эксплуатации. В результате может сложиться определенный дисбаланс: мощности, используемые для дешифрования, могут оказаться намного большими, чем мощности шифрования. По названным причинам растет интерес к совершенным шифрам, в том числе к одноразовому блокноту (шифру Вернама).

Одноразовый блокнот (ОБ) представляет собой набор однократно используемых ключевых последовательностей (страниц) размером не меньшим, чем длина шифруемого сообщения. Шифрование заключается в наложении ключа на открытый текст с помощью операции XOR. Шифр Вернама обладает двумя важными особенностями: абсолютной криптостойкостью (теоретически доказанной для истинно случайной ключевой последовательности) [2] и более высокой по сравнению с другими шифрами скоростью работы. Последнее свойство ОБ достигается за счет предельной простоты алгоритма шифрования и разделения во времени подготовки шифроблокнота и самого процесса шифрования. Это является серьезным преимуществом при работе в системах реального времени, к которым относится БЛА. При практической реализации такого шифрования наиболее сложной задачей является создания ключа (шифроблокнота), который должен представлять собой последовательность равновероятных, не зависящих друг от друга символов. В настоящее время активно используются и развиваются как подходы, основанные на классических генераторах

псевдослучайных последовательностей, так и новые варианты генерации с применением квантовых, фрактальных, нейросетевых, генетических и других биоинспирированных алгоритмов [3–6]. Проводятся также теоретические исследования, расширяющие в определенных условиях область доказательной абсолютной стойкости ОБ [7].

Технические вопросы, связанные с быстрой генерацией качественного шифроблокнота большого объема, его хранения и передачи на БЛА, в настоящее время успешно разрешаются за счет использования мощных и доступных графических процессоров (распараллеливание процессов), современных быстрых флэш-накопителей.

Анализ текущего состояния в области исследований и применения ОБ показывает, что такая система шифрования жизнеспособна, активно развивается и имеет хорошие перспективы применения в будущем.

СПИСОКЛИТЕРАТУРЫ

1. Bernstein D.J., Lange T., Niederhagen R. Dual EC: A Standardized Back Door. / In: Ryan P., Naccache D., Quisquater JJ. (eds) The New Codebreakers. Lecture Notes in Computer Science. – Berlin: Springer, 2016. Vol. 9100. P 256-281.
2. Shannon C.E.Communication theory of secrecy systems // Bell Syst. Tech. J. 1949. Vol. 28. P. 656–715.
3. БурловС.А., ГороховА.В. О возможности защиты квантового канала связи на состояниях орбитального углового момента фотонов // Сб. тр. конф. «Актуальные проблемы обеспечения информационной безопасности». 2017. С. 69-73.
4. Кулешов С.В. Фрактальное шифрование // ТРУДЫ СПИИРАН. 2004. Том 1. №2. С. 231-235.
5. ЮрьевР.А. Обзормоделейнейрокриптографии // Вестникнаучныхконференций. 2015. № 4-2 (4). С. 160-164.
6. СергеевА.С. Применениебиоинспирированныхинформационныхтехнологийдлярешениязадачклассического, асимметричногоиблочногокриптоанализа // Сб. материаловXIМеждународнойконф. Понеравновеснымпроцессамвсоплахиструях (NPNJ'2016). 2016. С. 457-459.
7. Ryabko B.The Vernam cipher is robust to small deviations from randomness // Problems of Information Transmission. 2015. Vol. 51.No. 1.P. 82-86.

УДК 004.056.53

ОСНОВНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СКЛАДА, РАБОТАЮЩЕГО ПОД УПРАВЛЕНИЕМ WMS-СИСТЕМЫ

Губа Евгений Александрович
Россия, Санкт-Петербург, Кронверкский пр., 49
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mail: temarual@gmail.com

Аннотация. Вработе рассмотрены наиболее частые угрозы для информационной безопасности склада, работающего под управлением WMS-системы, а также последствия их реализации.

Ключевые слова: *информационная безопасность; система управления складом; угроза.*

MAJOR THREATS OF INFORMATION SAFETY OF THE WAREHOUSE, WORKING UNDER THE MANAGEMENT OF THE WMS-SYSTEM

Guba Evgeny
Russia, St. Petersburg, Kronverksky pr.,49
ITMO University,
e-mail: temarual@gmail.com

Abstract. The paper considers the most frequent threats to the information security of the warehouse operating under the control of WMS-system, as well as the consequences of their implementation.

Keywords: *information security; warehouse management system; threat.*

С развитием информационных технологий организации все больше используют электронные управление и учет своих активов, уходя от использования бумажных носителей информации. И это также коснулось учета и движения товарно-материальных ценностей, хранимых на складах. Система управления складом (СУС) или WMS-система (от английского Warehouse Management System) - информационная система, обеспечивающая автоматизацию управления бизнес-процессами работы складского комплекса организации.

Помимо ряда преимуществ, которое дает использование WMS-системы, также возникают различные угрозы для информации, занесенной в СУС, и трудности по обеспечению ее безопасности. Нарушение трех главных аспектов ИБ: целостности, доступности и конфиденциальности – может быть очень критичным для организации.

Рассмотрим основные угрозы информационной безопасности, которой может быть подвержена складская система.

В зависимости от специфики склада к системе управления складом предъявляются различные требования. Если склад прикреплен, например, к оборонному производству, то обеспечение

конфиденциальности будет важным пунктом в организации защиты информации, так как по номенклатурным позициям можно определить состав изготавливаемых изделий и другие различные характеристики. Если в базе данных WMS-системы не содержится различного рода конфиденциальная информация, то обеспечение конфиденциальности данных не будет являться значимым направлением. Без целостности и доступности в принципе невозможна работа WMS-системы.

На сегодняшний день в большинстве складов для удобства работы используется беспроводная сеть. WMS-системы с применением беспроводных сетей обеспечивают высокую скорость выполнения действий работников склада, снижают вероятность проявления ошибок при ручном вводе и максимально автоматизируют учет товарно материальных ценностей организации. Но произведенные при настройке и развертывании сети ошибки, могут позволить внешним злоумышленникам беспрепятственно проникнуть в сеть. Самой грубой ошибкой на многих предприятиях является использование уязвимого протокола безопасности. Для обеспечения защиты беспроводной сети применяются специализированные протоколы. Эти протоколы будут обеспечивать доступ к сети только тем, кто действительно нуждается в доступе, а также передавать данные только в зашифрованном виде.

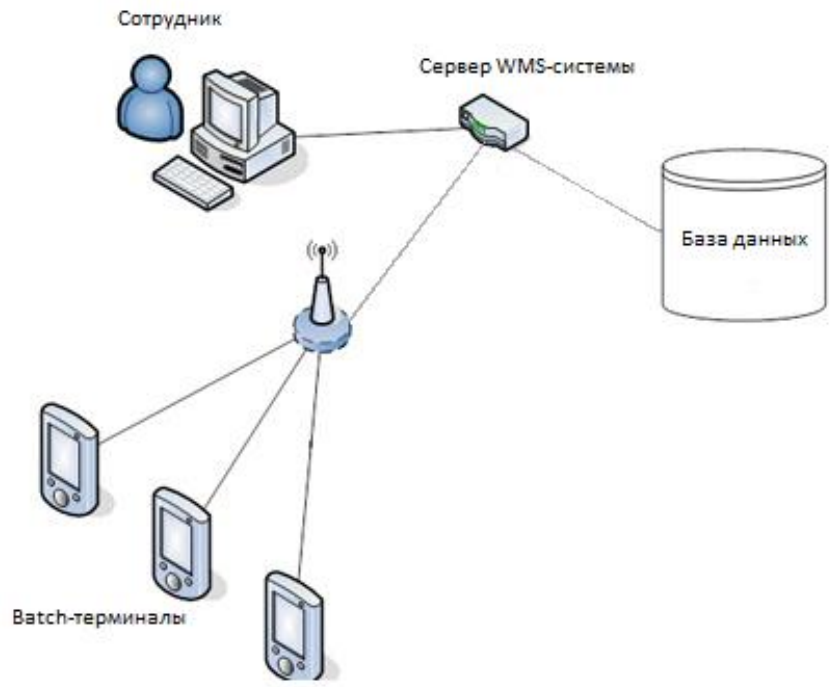


Рис. 1. Типовая схема организации WMS-системы

Основную угрозу информационной безопасности носят сами сотрудники. Это является следствием низкой компьютерной грамотности и банального непонимания важности и ценности информации, с которой они работают.

Самое распространённой причиной нарушения информационной безопасности является использование стандартного или слабого пароля для учетных записей работников. Зачастую пароль, выданный при регистрации, так и не меняется в процессе работы. То есть получается ситуация, когда большинство работников имеют одинаковый пароль. В таком случае злоумышленнику совсем не составляет труда авторизоваться от имени кого-нибудь из числа персонала.

Слабое дифференцирование прав доступа, ввиду взаимозаменяемости сотрудников, также носит угрозу нарушения целостности, доступности и конфиденциальности для информации. Не стоит забывать и об учетных записях сотрудников, которые уже не работают в организации. Их необходимо блокировать сразу после увольнения должностного лица.

Во избежание тяжелых последствий от нарушения информационной безопасности следует как можно чаще производить резервное копирование базы данных WMS-системы, так как именно там находится вся основная информация, необходимая для работы.

Результатом нарушения информационной безопасности склада, грозит от временной остановки работы склада (или производства, к которому прикреплен склад), до потери всей информации об остатках, числящихся на складе (потребуется проводить полную инвентаризацию), и становления известной этой информации третьим лицам.

Обеспечение информационной безопасности должно осуществляться непрерывно. В связи с этим необходимо принимать различные меры по противодействию возникновения различных угроз безопасности информации, хранящейся в складской системе.

СПИСОК ЛИТЕРАТУРЫ

1. Куломиец Б.Н., Кукарцев В.В. Проблемы информационной безопасности склада и пути их решения // Технические науки. 2015. №33-1 [Электронный ресурс]. URL: http://novainfo.ru/article/3421 (дата обращения: 21.09.2017).

УДК 007

МОДЕЛИРОВАНИЕ ОРГАНИЗМА ЧЕЛОВЕКА ДЛЯ ПОДДЕРЖКИ ВРАЧЕБНЫХ РЕШЕНИЙ

Губин Александр Вадимович[1], Игнатьев Михаил Борисович[2], Катермина Татьяна Сергеевна[3], Красников Андрей Георгиевич[4]
[1]РНЦ «Восстановительной травматологии и ортопедии» им.академика Г.А.Илизарова
Россия, г. Курган, ул. М. Ульяновой, 6
[2]Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, Большая Морская ул., 67
[3]Нижневартовский государственный университет
Нижневартовск, Ханты-Мансийский автономный округ,ул. Ленина, 56
[4]Первый медицинский университет им. И.П. Павлова
Санкт-Петербург, ул. Льва Толстого, 6-8
e-mails: gubin_av@ilizarov.ru, ignatmb@mail.ru

Аннотация. Рассматривается проблема компьютерного моделирования организма человека и определяется его стратегия – от моделирования на уровне органов до моделирования на молекулярном уровне.

Ключевые слова: *лингво-комбинаторное моделирование; сложность; поддержка врачебных решений; моделирование живой клетки; молекулярный уровень.*

SIMULATION OF THE HUMAN BODY TO SUPPORT MEDICAL DECISIONS

Gubin Alexander[1], Ignatiev Mikhail[2], Katerina Tatiana[3], Krasnikov Andrey[4]
[1]Russia, Kurgan,640014, "Russian Ilizarov Scientific Center "Restorative traumatology and Orthopaedics"
,[2]St. Petersburg state University of aerospace instrumentation
[3]Nizhnevartovsk state University, [4]St. PetersburgPavlov First Medical University
e-mails: gubin_av@ilizarov.ru, ignatmb@mail.ru

Abstract. Considers the problem of computer simulation of the human body and is defined by its strategy – from modeling at the level of the organs to the simulation at the molecular level.

Keywords: *linguo-combinatorial simulation; complexity; support medical decisions; modeling of a living cell; the molecular level.*

В настоящее время для исследования и создания сложных систем и сооружений широко применяется компьютерное моделирование. По мнению Всемирной организации здравоохранения (ВОЗ) необходимо развивать компьютерное моделирование и в медицине, прежде всего чтобы уменьшить количество врачебных ошибок. Но возникает вопрос – на каком уровне строить эти компьютерные модели? Это возможно и на молекулярном уровне.

Например, в 2012 году ученым Стенфордского университета удалось создать полную модель живого организма, использовав данные 900 научных работ, для того, чтобы учесть все молекулярные взаимодействия, происходящие в жизненном цикле бактерии Mycoplasma genitalium – одного из самых маленьких организмов, способных существовать самостоятельно. Был создан весь живой организм in silico – на кремнии – с помощью компьютерной модели, что позволяет ставить различные эксперименты, проведение которых технически неосуществимо в случае живой клетки. А как быть с человеческим организмом, с многоклеточным организмом?

Эта задача по сложности превосходит задачу моделирования бактерии в миллиарды раз, конечно со временем и она будет решена, а как быть сейчас? Еще в 2000 году мы предложили моделировать основные органы человека и их взаимодействие [1] , для лечащего врача важно рассматривать организм прежде всего на уровне органов и мы предложили построить лингво-комбинаторную модель организма исходя из общепринятого набора органов: органы движения (кости, мышцы, связки), органы пищеварения, органы дыхания, мочеполовые органы, кроветворная и лимфатическая системы, центральная нервная система, периферическая нервная система, железы внутренней секреции, кожа и сенсорные системы, иммунная система, -такие модели были построены и уже применяются.

В связи с разработкой электронного паспорта здоровья родилось предложение сделать его основой конкретную лингво-комбинаторную организма [2].

СПИСОК ЛИТЕРАТУРЫ

1. Ignatyev M.B. et al. Global model of organism for decision making support: Proc.of the high performance computing symp.HPC 2000/Ed. A.Tentner. Washington D.C., USA, 2000, P. 66-71.
2. Игнатьев М.Б. Кибернетическая картина мира. Сложные киберфизические системы, СПб, 2014, 478 стр.

УДК 004.054

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ BIGCODEДЛЯ ОЦЕНКИ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Заколдаев Данил Анатольевич[1], Римша Андрей Сергеевич[2], Югансон Андрей Николаевич[1]
[1]Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
[2]Тюменский государственный университет
Россия, Тюмень, ул. Володарского, 6
e-mails: d.zakoldaev@mail.ru, rimshaandrew@gmail.com, a_yougusnon@corp.ifmo.ru

Аннотация. В статье рассмотрены вопросы оценки надежности программного обеспечения. Предлагается использование технологии BigCode для повышения качества оценивания. Данная технология находится на стыке машинного обучения, программной инженерии, языков программирования и обработки естественных языков. Приведены достоинства и недостатки использования технологии BigCode на ранних этапах разработки программного обеспечения. Описаны перспективы применения.

Ключевые слова: *BigCode; структурированные и неструктурированные данные; технологическая безопасность исходных кодов; надежность программного обеспечения; анализ исходных кодов.*

USING BIG CODE FOR ASSESS OF SOFTWARE RELIABILITY

Zakoldaev Danil[1], Rimsha Andrei[2], Iuganson Andrei[3]
[1]ITMO University
Russia, St. Petersburg, Kronverkskiy pr., 49
[2]University of Tyumen
Russia, Tyumen, Volodarskogo str., 6
[3] ITMO University
Russia, St. Petersburg, Kronverkskiy pr., 49
e-mails: d.zakoldaev@mail.ru, rimshaandrew@gmail.com, a_yougusnon@corp.ifmo.ru

Abstract. A new technology for calculation of assess for software tecurity was described in this article. The Big Code technology was introduced to increase the quality and accuracy of assess. This technology appeared as a result of convergence of the following studies: machine learning, software engineering, programming languages, natural language processing. Advantages and disadvantages of using the Big Code were presented. The prospects of application were specified.

Keywords: *Big Code; structured and nonstructured data; sourcecode tecurity; software reliability; sourcecode analysis.*

Современные стандарты по разработке промышленного программного обеспечения подразумевают главенствование вопроса обеспечения надежности функционирования программного обеспечения над оценкой надежности. Парадокс заключается в том, что для должного обеспечения уровня надежности функционирования разработанного программного обеспечения, необходимо однозначно определять этот уровень. На сегодняшний день в отрасли не принят единыйстандарт по оценке надежности.

Проблема обеспечения надежности программных продуктов стала одним из важнейших приоритетов мирового экономического развития, эффективным средством решения социальных задач. В цивилизованных государствах сложилась развитая система технического законодательства, не просто устанавливающая конкретные обязательные требования к качеству программного обеспечения, но нацеленная на то, чтобы эти требования были финансово и экономически обоснованы.

Оценка надёжности программных средств представляет собой совокупность операций, включающих выбор номенклатуры показателей надежности оцениваемого программного средства, определение значений этих показателей и сравнение их с базовыми значениями.

В настоящее время растет число свободно распространяемых программных средств высокого качества. Такие программы можно выделить в отдельный класс данных – исходные коды программного обеспечения. GitHub – крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки. Наличие большого количества исходных текстов в свободном доступе позволяет разрабатывать новые инструменты для анализа статистических зависимостей.Такие

инструменты позволят извлекать полезную информацию из существующих баз с исходными текстами и использовать эту информацию для решения широкого круга вопросов, в том числе, оценки надежности программного обеспечения

Технология BigCode представляет из себя совокупность подходов, инструментов и методов обработки структурированных и неструктурированных данных, представляющих из себя исходные коды программных обеспечений для получения воспринимаемых человеком результатов. К задачам, решаемым с помощью технологии BigCode, можно отнести предсказание поведения программы, предсказание имен идентификаторов переменных, и даже программных багов. Использование технологии BigCode предполагает кросс-дисциплинарные исследования в области машинного обучения (MachineLearning), программной инженерии (SoftwareEngineering), языков программирования (Programming Languages), обработки естественных языков (Natural language processing)[1].

На сегодняшний день существуют следующие решения, использующие технологии BigCode:

1) Автоматическое завершение исходных кодов на языке JavaScript. Цель данного решения – разработать инструмент, который может предсказать дальнейший код на языке JavaScript. Первая задача – предсказание программного интерфейса приложения, вторя – завершение произвольных программных элементов числовыми и строковыми константами.

2) Определение сходства фрагментов исходных кодов. Сходство исходных кодов является центральным вопросом в таких сферах, как поиск плагиата, автоматический перевод, обучение программированию. Цель данного решения – определение закономерностей между различными фрагментами исходных кодов программ, используя технологию семантических связей.

3) Изучение закономерностей наименования идентификаторов методов и переменных. Цель данного решения – разработать систему, способную предугадать имя метода. Как известно, разработчики называют свои переменные, классы и методы исходя из контекста решаемой задачи. Выявление закономерностей в названии методов является важной и тяжелой задачей для машинного обучения и является первым шагом на пути определения функциональности программы с точки зрения искусственного интеллекта.

4) Поиск статистических закономерностей в исходных кодах программ. Цель данного решения – разработать инструмент, позволяющий осуществлять поиск конкретных процедур на языке ассемблера. Инструмент представляет возможность находить семантически схожие небольшие линейные фрагменты кода [2].

Отдельно стоит отметить работу [3], в которой авторы спроектировали масштабируемую систему, названную JSNice, решающую следующие задачи (для языка JavaScript):

– прогнозирование имен идентификаторов (синтаксическое);
– прогнозирование типов данных по именам переменных (семантическое).

На рис. 1 представлено статистическое прогнозирования основных параметров исходных текстов.

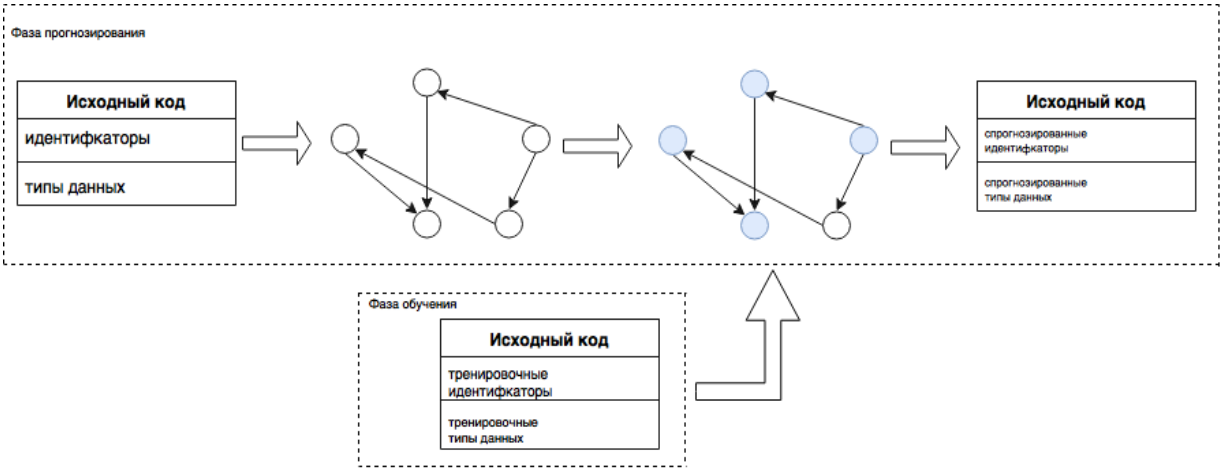


Рис. 1. Статистическое прогнозирование основных параметров исходных текстов

Процедура прогнозирования состоит из двух фаз: фаза прогнозирования и фаза обучения. В первой фазе, исследуемый исходный код попадает на вход алгоритма, преобразуется в так называемую сеть зависимостей. Ее предназначение – установить связи между прогнозируемыми параметрами и известными. Далее, данная сеть обрабатывается исходя из сведений, полученных на фазе обучения (основные зависимости идентификаторов и типов данных, имена идентификаторов и т.д.) и преобразуется в исходный код с подобранными параметрами.

Использование технологии BigCodeдля оценки надежности программных средств может существенно повысить качество таких оценок, благодаря большой высококачественной

репрезентативной базе исходных текстов, используемых при анализе. Здесь стоит отметить Software Heritage – проект Французского института исследований в информатике и автоматике, задачей которого является сбор, сохранение и предоставление доступа к исходным текстам, собранным в одном месте из различных доступных источников.

На рис. 2 представлена методика расчета оценки надежности программного обеспечения.

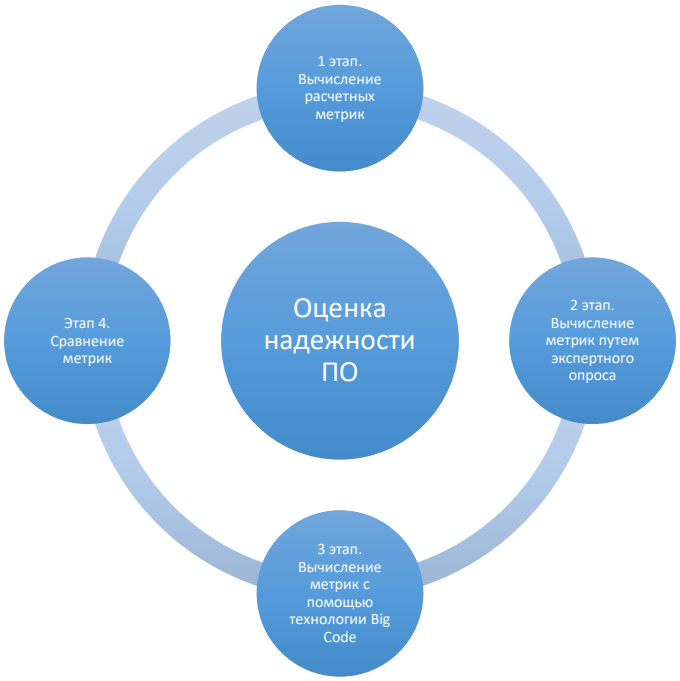


Рис. 2. Методика расчета оценки надежности программного обеспечения

Предлагаемая методика содержит следующие этапы:

1. На первом этапе происходит вычисление расчетных метрик. Данный этап подразумевает определение таких метрик, как показатель устойчивости к искажающим воздействиям, вероятность безотказной работы, оценка по среднему времени восстановления, оценка по продолжительности преобразования входного набора данных в выходной.
2. На втором этапе дается оценка метрикам с помощью экспертного опроса.
3. Третий этап включает в себя использование технологии BigCode. В рамках данного этапа происходит следующее: строится вероятностная модель на основе большого объема исходных кодов. Затем данная модель используется для проверки метрик исследуемого исходного кода.
4. Четвертый этап – сравнение полученных метрик с соответствующими значениями аналога или программного средства, принимаемого за эталонный образец. В качестве аналогов выбираются реально существующие программные средства того же функционального назначения, что и сравниваемое программное обеспечение, с такими же основными параметрами, подобной структурой и применяемые в схожих условиях эксплуатации [4].

К достоинствам использования технологии BigCode для оценки надежности программного обеспечения можно отнести:

– обнаружение ошибок, связанных с неверным определением типа данных при разработке программного обеспечения (например, целочисленный тип данных вместо числа с плавающей запятой);

– обнаружение ошибок, связанных с недостатками спроектированных алгоритмов и методов обработки данных;

– большая выборка, позволяющая сравнить исследуемые функции исходного кода с аналогичными функциями свободно распространяемых программных средств;

– прогнозирование атрибутов разрабатываемых исходных текстов для минимизации вероятности возникновения ошибок на стадии проектирования.

Однако для вычисления метрик с помощью технологии Big Code требуется репрезентативная база данных исходных текстов, оптимальных для использования в рамках оценивания надежности программного обеспечения. Для этих целей подойдет проект Software Reliability Lab (ETH Zurich) совместно с Software Research Lab (Technion, Israel), названный «Learning from Big Code», который содержит выборки исходных текстов для следующих языков программирования: Python, JavaScript, Java, а также веб-фреймворка Django.

Заключение. Таким образом, в ходе исследования была предложена принципиально новая технология, позволяющая повысить качество оценки надежности программных средств.

Предложенная методика сложна в применении, так как требуют знаний таких характеристик ПО, которые можно вычислить только после длительной эксплуатации. Основываясь на данной работе, можно сделать вывод: отсутствует общее решение проблемы расчета оценки надежности программного обеспечения и существуют множество частных решений, которые не учитывают такие факторы как интенсивность внесения и устранения ошибок в программе [5].

Важным вопросом практического применения методики является подготовка исходных данных. Эта задача особенно актуальна при оценке на ранних этапах жизненного цикла. Исходные данные (общее количество ошибок и временные характеристики процессов их поиска и устранения) могут быть получены с использованием объектноориентированных метрик сложности и статистики, собранной при разработке похожих программных проектов, в том числе, с помощью использования технологии Big Code.

Тем не менее, использование представленной методики позволит повысить уровень качества автоматизированных систем управления различного назначения, а также минимизировать риски, связанные с отказом программного обеспечения на ранних стадиях эксплуатации. Данная методика будет использована при разработке научных и программных решений для расчета надежности программных средств.

СПИСОК ЛИТЕРАТУРЫ

1. Allamanis M. et al. A Survey of Machine Learning for Big Code and Naturalness //arXiv preprint arXiv:1709.06182. – 2017.
2. Bielik P., Raychev V., Vechev M. Programming with" Big Code": Lessons, Techniques and Applications //LIPIcs-Leibniz International Proceedings in Informatics. – Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2015. – Т. 32.
3. Veselin Raychev, Martin Vechev, Andreas Krause, Predicting Program Properties from "Big Code", Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, January 15-17, 2015, Mumbai, India [doi>10.1145/2676726.2677009]
4. Югансон А.Н., Заколдаев Д.А. Разработка методики для расчета оценки технологической безопасности программных средств // Вестник УрФО. Безопасность в информационной сфере - 2017. - № 1(23). - С. 20-23
5. Хунов Т.Х. Анализ моделей прогнозирования надежности программных средств // Новые информационные технологии в автоматизированных системах. 2016. №19. URL: http://cyberleninka.ru/article/n/analiz-modeley-prognozirovaniya-nadezhnosti-programmnyh-sredstv (дата обращения: 27.09.2017).

УДК 004.056

ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ НАЗЕМНОГО ГОРОДСКОГО ПАССАЖИРСКОГО ТРАНСПОРТА

Ильченко Лидия Михайловна[1], Зайцев Святослав Игоревич[2]
[1] Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
[2] Государственный университет морского и речного флота имени адмирала С.О. Макарова
Российская Федерация, Санкт-Петербург, ул. Двинская, 5/7
e-mails: Lidiya9510@yandex.ru, Sunilink@yandex.ru

Аннотация. В данной работе рассматриваются особенности построения системы защиты информации в автоматизированных системах управления наземного городского пассажирского транспорта.

Ключевые слова: *информационная безопасность; интеллектуальная дорожно-транспортная система; угрозы безопасности; средства защиты информации; автоматизированная система управления наземным городским пассажирским транспортом.*

PARTICULAR QUALITIESOF CONSTRUCTION OF INFORMATION PROTECTION SYSTEM IN INTELLECTUAL SYSTEMS OF GROUND CITY PASSENGER TRANSPORT

Ilchenko Lydia[1], Zaytsev Svyatoslav[2]
[1]St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverksky pr., 49
[2]Admiral Makarov State University of Maritime and Inland Shipping
Russia, St. Petersburg, Dvinskaya str., 5/7
e-mails: Lidiya9510@yandex.ru, Sunilink@yandex.ru

Abstract. In this paper we consider the construction of a system for protecting information in the intellectual systems of ground city passenger transport.

Keywords: *information security; intellectual road and transport system; security threats; data protection facilities; intellectual systems of ground city passenger transport.*

Введение. На сегодняшний день транспортная система является неотъемлемой частью инфраструктуры любого развитого государства. На территории России насчитывается более 1 396 000 км сети автодорог общего пользования. В связи с чем возникает ряд необходимостей, основной из которых является максимизация качества функционирования дорожно-транспортной

системы, которая особенно остро ощущающихся в больших городах, где поток транспортных средств намного превышает пропускную способность дорожной инфраструктуры.

Существует два направления решения этой задачи: использование технологий автоматизированного управления транспортной системой путем использования информационных технологий; и модернизация участков дороги.

Во время проектирования автономной информационной системы наземного транспорта, решающей отдельные задачи, появилась обоснованная необходимость в создании общей государственной стратегии развития, контроля и регламентации единого программно-аппаратного комплекса, объединяющего деятельность всех органов власти, действующих в сфере транспортной инфраструктуры государства [6].

Система, основной функцией которой стало объединение в единый технологический и технический комплекс множество отдельных подсистем дорожного движения, получила название «Интеллектуальная дорожно-транспортная система» (далее – ИТС) [5].

Одной из ведущих подсистем ИТС является система автоматизированного управления наземным городским пассажирским транспортом (АСУ НГПТ).

Стратегическую цель создания АСУ НГПТ составляет удовлетворение спроса на пассажирский транспорт. Результатом функционирования АСУ НГПТ является описание целевых направлений построения интеллектуальной дорожно-транспортной системы:

– мониторинг дорожной ситуации;
– организация транспортного потока и пр.

В рамках управления системой городского наземного транспорта рассматривается:

– управление непосредственно самим транспортом (автобусы, трамваи, и пр), частью пригородных перевозок (связь города с вокзалами и аэропортами);
– определение местоположения транспортных средств в режиме реального времени на базе технологий ГЛОНАСС/GPS;
– система информирования пассажиров на остановочных пунктах и в транспортных средствах;
– система учета пассажиров;
– система диспетчерского управления;
– система безопасности;
– дуальный канал связи транспортных средств с диспетчерскими центрами;

Основными функциями автоматизированной системы управления наземным городским пассажирским транспортом являются:

1. Диспетчеризация:
– журналирование выполненных работ;
– управление движением в режиме реального времени;
– контроль за соблюдением расписание [3].
2. Планирование:
– составление паспорта маршрута;
– мониторинг пассажиропотока;
– журналирование и аудит работы перевозчиков.
3. Безопасность:
– видеоконтроль;
– реагирование в случае поступления сигналов бедствия;
– информирование о чрезвычайных происшествиях [2, 4].

Основные угрозы безопасности информации АСУ наземного городского пассажирского транспорта представлены в таблице 1 [8].

Таблица 1

Потенциальные угрозы безопасности информации автоматизированной системы наземного городского пассажирского транспорта

Способы нанесения ущерба	Объекты воздействия			
	Оборудование	Программы	Данные	Персонал
Нарушение конфиденциальности данных	1.1 Хищение физических носителей информации, подключение к сетям линии связи, несанкционированное использование ресурсов	1.2 Копирование данных, перехват.	1.3 Хищение, копирование, перехват.	1.4 Разглашение сведений о защите АСУ, халатность сотрудника.
Нарушение	2.1 Подключение,	2.2 Внедрение	2.3 Искажение,	2.4

Способы нанесения ущерба	Объекты воздействия			
	Оборудование	Программы	Данные	Персонал
целостности данных	модификация, изменение режимов работы, несанкционированное использование ресурсов.	аппаратных закладок, вирусов и «троянов».	модификация	Человеческий фактор
Нарушение работоспособности АСУ	3.1 Изменение режимов функционирования, выход из строя, хищение, разрушение.	3.2 Искажение, подмена, удаление	3.3 Искажение, удаление, ложные данные.	3.4 Ошибки сотрудника

Актуальными являются угрозы: 1.1, 1.3, 1.4, 2.1-2.4, 3.1, 3.3. Для автоматизированной системы управления главными векторами обеспечения защиты является доступность и целостность. Конфиденциальность данных обеспечивается по необходимости [9].

В качестве источников внутренних отказов автоматизированной системы управления выступают:

– непреднамеренные ошибки эксплуатации системы;
– системные ошибки из-за превышение допустимых объемов обрабатываемых данных;
– отказ программного и (или) аппаратного обеспечения;
– потеря информации и (или) физических носителей информации [1].

Для рассматриваемой системы класс защищенности определяется в соответствии с приказом ФСТЭК России от 14 марта 2014 г. № 31, и напрямую зависит от уровня значимости обрабатываемых данных, который прямо пропорционален возможному ущербу для каждого из свойств безопасности информации (целостности, доступности, конфиденциальности).

Степень возможного ущерба для АСУ наземного городского пассажирского транспорта:

1. Для целостности – низкая.
2. Для доступности – низкая.
3. Для конфиденциальности – низкая.

Исходя из вышеуказанных данных уровень значимости системы соответствует третьему (УЗ-3), а класс защищенности, в соответствии с таблицей в п.3 Приложения №1 приказа ФСТЭК России от 14 марта 2014 г. № 31, соответствует третьему классу (К3).

Обеспечение защиты информации в АСУ наземного городского пассажирского транспорта достигается за счет комплексного подхода к организации системы защиты данных. Базовый набор мер представлен в приложении №2 приказа ФСТЭК России от 14 марта 2014 г. №31. Адаптивный набор мер формируется в результате оценки угроз информационной безопасности на базе составленной модели угроз.

Как минимум, меры защиты должны обеспечивать минимизацию, либо полную ликвидацию угроз безопасности информации, источником которых является нарушитель с низким потенциалом.

В системе защиты должны быть реализованы следующие группы мер:

– идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);
– управление доступом субъектов доступа к объектам доступа (УПД);
– ограничение программной среды (ОПС);
– защита машинных носителей информации (ЗНИ);
– регистрация событий безопасности (РСБ);
– антивирусная защита (АВЗ);
– обнаружение (предотвращение) вторжений (СОВ);
– контроль (анализ) защищенности информации (АНЗ);
– целостность автоматизированной системы управления и информации (ОЦЛ);
– доступность технических средств и информации (ОДТ);
– защита среды виртуализации (ЗСВ);
– защита технических средств и оборудования (ЗТС);
– защита автоматизированной системы и ее компонентов (ЗИС);
– безопасная разработку прикладного и специального программного обеспечения (ОБР);
– управление обновлениями программного обеспечения (ОПО);
– планирование мероприятий по обеспечению защиты информации (ПЛН);
– обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС);
– информирование и обучение персонала (ИПО);
– анализ угроз безопасности информации и рисков от их реализации (УБИ);
– выявление инцидентов и реагирование на них (управление инцидентами) (ИНЦ);

– управление конфигурацией автоматизированной системы управления и ее системы защиты (УКФ).

Исходя из анализа Реестра сертифицированных ФСТЭК России средств защиты информации и практики их применения, можно составить перечень необходимых и достаточных средств защиты:

– СЗИ от несанкционированного доступа (СЗИ от НСД);
– средств индивидуального межсетевого экранирования (МЭ);
– средств обнаружения вторжений (СОВ);
– средств защиты виртуализации (СЗВ);
– средств резервирования (резерв.коп);
– средств антивирусной защиты информации (АВЗ).

А также средства криптографической защиты информации, сертифицированные Федеральной службой безопасности РФ (ФСБ России).

Третий класс защищенности предъявляет следующие требования:

– средства вычислительной техники не ниже 5 класса;
– СЗИ не ниже 6 класса [7].

Общий перечень средств защиты информации и их функционал представлен в таблице 2.

Таблица 2

Реализация функциональных комплексов

№ п/п	Усл. обознач.	СЗИ от НСД	СЗВ	МЭ + IDS	АВЗ	Резерв. Коп.	СКЗИ	Орг. меры
1.	ИАФ	+	+					
2.	УПД	+	+	+				
3.	ОПС	+	+					
4.	ЗНИ							+
5.	РСБ	+	+	+	+		+	
6.	АВЗ				+			+
7.	СОВ			+				
8.	АНЗ	+		+				+
9.	ОЦЛ	+	+	+	+	+	+	
10.	ОДТ					+		+
11.	ЗСВ		+					+
12.	ЗТС							+
13.	ЗИС	+		+	+	+	+	
14.	ОБР							+
15.	ОПО	+			+			+
16.	ПЛН							+
17.	ДНС					+		+
18.	ИПО							+
19.	УБИ							+
20.	ИНЦ	+	+	+	+		+	+
21.	УКФ							+

Выводы. При проектировании системы защиты необходимо учитывать все особенности АСУ НГПТ, а также необходимо учитывать актуальные угрозы безопасности и специфику обрабатываемых данных, акцентируя внимание на доступности и целостности обрабатываемой информации, и лишь по необходимости на конфиденциальности.

Кроме этого, необходимо учитывать требования нормативно-правовых актов, регламентирующих данную категорию автоматизированных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2014. – 594 с.
2. Жанказиев. С.В. Интеллектуальные транспортные системы: учеб. пособие / – М.: МАДИ, 2016. – 120 с.
3. Ивченко Б.П., Мартыщенко Л.А., Монастырский М.Л. Теоретические основы информационно-статистического анализа сложных систем. – СПб.: Лань, 1997. – 320 с.
4. Коноплянко, В.И. Организация и безопасность дорожного движения / В.И. Коноплянко. – М.: Транспорт, 1991. – 183 с.
5. Косолапов, А.В. Повышение эффективности информационного обеспечения участников дорожного движения в городах: дис. …канд. техн. наук. – М., 1992.
6. Опыт создания и эксплуатации интеллектуальных транспортных систем: Информационный сборник / Федеральное дорожное агентство Министерства транспорта Российской Федерации. – М.: ООО «Принт Форс Паблишинг», 2009. – 287 с.
7. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных

объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». – 42 с.
8. Руководящий документ «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», от 18 мая 2007 года, ФСТЭК России.
9. Руководящий документ «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры», от 18 мая 2007 года, ФСТЭК России.

УДК 004.05

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК СПОСОБ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СВЕДЕНИЯМ, СОСТАВЛЯЮЩИМ КОММЕРЧЕСКУЮ ТАЙНУ

Кизрякова Анастасия, Солодовников Владислав
Университет ИТМО,
Россия, Санкт-Петербург, Кронверский пр., 49
e-mails: anastasia.kiz6@gmail.com, solsaturate@gmail.com

Аннотация. В данной статье был рассмотрен пример несанкционированного доступа к сведениям, составляющим коммерческой тайне. Представлены различные способы социальной инженерии актуальные на данный момент. Основная идея статьи заключается в необходимости принятия мер по защите информации от социальной инженерии, проведения инструктажей и обучения персонала для предостережения от случаев утечки конфиденциальной информации.

Ключевые слова: *социальная инженерия; коммерческая тайна; информационная безопасность.*

SOCIAL ENGINEERING AS A METHOD OF UNAUTHORIZED ACCESS TO THE INFORMATION CONCERNING THE TRADE SECRET

Kizryakova Anastassiya, Solodovnikov Vladislav
St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverksky pr., 49
e-mails: anastasia.kiz6@gmail.com, solsaturate@gmail.com

Abstract. In this article, an example of unauthorized access to information constituting a trade secret was considered. Presented are various ways of social engineering relevant at the moment. The main idea of the article is the need to take measures to protect information from social engineering, conduct briefings and train staff to prevent cases of leakage of confidential information.

Keywords: *social engineering; trade secret; information security.*

Коммерческая тайна является одной из важнейших активов организации. Информация может быть сокрыта и отнесена к коммерческой тайне в случае, если существуют обстоятельства, при которых можно увеличить доходы организации, избежать неоправданных расходов, сохранить конкурентоспособность на рынке товаров или принести иную коммерческую выгоду компании.

Поскольку на данный момент не существует организации, которая бы функционировала без помощи людей, всегда присутствует влияние человеческого фактора на внутриорганизационные процессы. В том числе и на процессы обеспечения защиты конфиденциальной информации. Человеческий фактор – термин, описывающий ошибочные действия людей в конкретных ситуациях, повлёкших за собой убытки. Такие действия могут быть как умышленными, так и неумышленными. К умышленным, как правило, относят действия сотрудников с целью получить выгоду, отомстить. К неумышленным можно отнести потеря носителей информации, уничтожение, искажение, открытие информации по неосторожности. К неумышленным действиям так же относится неосознанная «помощь» злоумышленниками, то есть социальная инженерия. Действия основаны на доверии сотрудника злоумышленнику, при этом сотрудник не осознаёт, что нарушает режим коммерческой тайны, в то время как, злоумышленник четко знает, что нарушает режим.

Социальная инженерия – это метод получения незаконного доступа к информации или средствам хранения информации без использования технических средств. Данный метод основан на использовании человеческого фактора, эмоций и является достаточно результативным для злоумышленника. Правонарушитель получает информацию о служащих объекта будущей атаки путем проникновения в организацию под видом штатного служащего или с помощью обычного звонка. Злоумышленник может представиться сотрудником технической службы и сославшись на возникновение некоторых проблем, выведать пароли.

Социальной инженерией стали интересоваться и ученые. Американский физик Ричард Фейнман славился тем, что мог открыть любой сейф, не взламывая его. Применяя знания человеческой психологии, он подбирал пароль, или же просто находил его в кабинете, записанным на листке бумаги [5].

Существуют различные техники социальной инженерии, все они основаны на техниках использующие когнитивные искажения. Когнитивные искажения – это отклонения в поведении,

мышлении человека, основанные на дисфункции убеждений. Такие отклонения могут приводить к неточности суждений и нелогичности действий. Эти уязвимости используются для атак, направленных на получение конфиденциальной информации, часто это происходит с согласия сотрудника компании.

Все техники применения социальной инженерии основаны на действиях после принятия решений людьми.

Претекстинг представляет собой набор действий, как правило, отработанных по заранее придуманному сценарию. В результате атаки жертва должна сделать определенные действия или выдать конфиденциальную информацию. Чаще всего данный вид атак применим к телефонным разговорам или средствам связи подобным программе Skype. В данном случае злоумышленнику нужно провести предварительные исследования и узнать некоторые данные о жертве, например, данные персонализации. С их помощью злоумышленник может войти в доверие жертвы и получать уже необходимую ему информацию.

Обратная социальная инженерия – социально-инженерная атака, в которой атакующий создает ситуацию, где жертва сталкивается с проблемой, и просит атакующего о помощи. Другая форма обратной социальной инженерии переводит стрелки на атакующего. Цель распознает атаку и использует психологические приемы, чтобы узнать, как можно больше информации об атакующем, чтобы бизнес мог направленно охранять свое имущество.

Фишинг – техника интернет-мошенничества, при котором злоумышленник получает нужные ему данные. Самая распространённая фишинговая атака: злоумышленник рассылает письма на электронную почту, которые выглядят как официальные письма от банка или платежной системы. В письме находятся форма для ввода персональных данных, либо ссылка на сайт с такой формой. На данный момент фишинг является самой популярной атакой социальной инженерии.

К примеру, сотрудник компании стал жертвой фишинг атаки. Пароль на некотором сайте получили третьи лица. После этого оказывается, что пароль совпал с тем, который используется в компании. Тут уже может возникнуть реальная угроза самой организации.

По данным, предоставленным компанией Gartner, сумма денежных средств, потерянных из-за фишинга в 2007 году в США, превысила отметку в 3 миллиарда долларов [6]. Это является наглядным показателем реальных убытков.

Так же, существует еще и телефонный фишинг – вишинг. В данном случае атака производится с помощью заранее записанных голосовых сообщений, которые в комплексе пытаются воссоздать технологию IVR систем.

Квид про кво является техникой, при которой злоумышленник, применяя свое актерское мастерство, представляется сотрудником технической поддержки и сообщает о возникновении технических неполадок или проблем. В ходе разговора атакующий желает получить контроль над компьютером жертвы.

Троянский конь – атака социальной инженерии, которая основывается на эмоциях людей, таких как: любопытство, страх, алчность. На электронную почту жертвы приходит письмо с информацией о выигрыше в лотерею, компроматом на знакомых людей и другим подобным содержанием. Во вложении письма находится вредоносная программа, которая после запуска может получить доступ к сведениям на компьютере или изменении информации злоумышленником.

Адаптацией троянского коня является «дорожное яблоко». Метод заключается в использовании инфицированных физических носителей. Носители могут быть оставлены в местах общественного пользования и снабжены официальными логотипами компаний. Люди вставляют носители в компьютер и запускают для удовлетворения своего любопытства.

Плечевой серфинг включает в себя сбор личной, конфиденциальной информации путем наблюдения за жертвой через плечо.

В 2012 году было проведено исследование среди специалистов информационных технологий согласно которому:

– 85 % опрошенных специалистов признались, что видели конфиденциальную информацию, которую им не положено было знать;

– 82 % признались, что информация, отображаемая на их экране, могла быть видна посторонним лицам;

– 82 % слабо верят в то, что в их организации сотрудники будут защищать свой экран от посторонних лиц.

Уязвимое место социальной инженерии в том, что злоумышленник является для собеседника темной лошадкой, поскольку он не знаком с ним лично.

Поэтому жертвам атак стоит использовать дополнительные меры безопасности воспользоваться ID, или телефоном с определителем номера. При обратной социальной инженерии у злоумышленника больше вероятности расположить к себе человека, поскольку это сам сотрудник компании обращается к правонарушителю за советом.

При успешно совершенном нападении, злоумышленник имеет доступ к конфиденциальной информации, в том числе сведениям, составляющим коммерческую тайну.

Утечка таких сведений может понести за собой немалые убытки. Не смотря на имеющийся режим коммерческой тайны и введенные меры безопасности, риск утечки информации присутствует всегда.

Основной метод противодействия социальной инженерии - обучение сотрудников, предупреждение о существующих методах несанкционированного доступа. Сотрудники должны четко понимать какую информацию не следует разглашать даже «техническому персоналу», а так же определять ложную информацию.

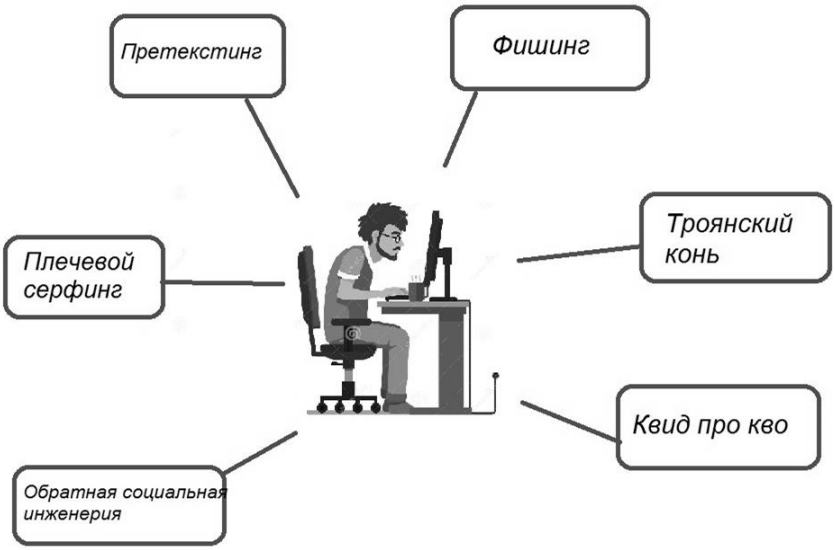


Рис. 1 Основные методы социальной инженерии

Меры по защите информации от атак социальной инженерии достаточно просты:

– сотрудники должны быть проинформированы, как нужно вести себя с клиентами и персоналом;

– пароли являются собственностью компании и не могут быть использованы в личных целях;

– по телефону нужно раскрывать только действительно необходимую информацию, если возникает сомнение в предоставляемой информации, стоит установить личный контакт с собеседником;

– раскрытие информации при личном общении так же требует раскрытия только нужной информацию;

– организация структурированного хранилища информации, все данные должны быть четко разделены по степени важности, недопустимо хранение важных и базовых документов в одном месте;

– разграничение доступа должно быть четко определено;

– ужесточение правил и инструкций по использованию важной информации;

– на рабочих компьютерах должно быть как можно меньше информации;

– обязательное использование антивирусов, программного обеспечения, осуществляющего сканирование и удаление вирусов на рабочих компьютерах.

Защита от социальной инженерии обязательно должна быть учтена в пользовательском интерфейсе информационной системы. Пользовательский интерфейс должен быть таким, чтобы минимизировать количество ошибок пользователя в результате воздействия на него социальной инженерии [5].

Большинство сотрудником пренебрегает данными мерами безопасности, забывают о том, какой уровень ответственности возложен на них при подписании обязательств о неразглашении сведений, составляющих коммерческую тайну, что влечет за собой возможные потери уже в денежном эквиваленте для организации.

Компании могут тратить большие финансовые средства на обеспечение информационной безопасности техническими методами.

Однако, если персонал не будет соблюдать нужные меры безопасности, не будет проинструктирован и будет подвержен атакам социальных инженеров, а службы безопасности не будут проверять бдительность персонала, никакие технические средства не помогут обеспечить нужный уровень защиты информации.

Выводы. После анализа способов социальной инженерии можно сделать вывод о том, что следует применять дополнительные способы зашиты информации, помимо стандартных.

Создание данных методов должно включать в себя четкое разграничение доступа, разработка системы инструкций и правил для персонала, ужесточение программной защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. Кевин Митник и Уильям Саймон Искусство обмана 2001.
2. European Visual Data Security.Visual Data Security White Paper 2014.
3. Википедия: сайт. - URL: https://ru.wikipedia.org/wiki/Социальная_инженерия.
4. Ричард Фейнман. Радость познания (The Pleasure Of Finding Things Out). — М.: АСТ, 2013. — 348, [4] с. — ISBN 978-5-17-078430-1.
5. Попов А.А. Эргономика пользовательских интерфейсов в информационных системах: учебное пособие / А.А. Попов. М.: РУСАЙНС, 2016. 312с.
6. Gartner: сайт. - URL: http://www.gartner.com/newsroom/id/565125.

УДК 004.05

МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ КАК СПОСОБ ПОЛУЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Кизрякова Анастасия, Солодовников Владислав
Университет ИТМО
Россия, Санкт-Петербург, Кронверский пр., 49
e-mails: anastasia.kiz6@gmail.com, solsaturate@gmail.com

Аннотация. Работа посвящена социальной инженерии как способу доступа к защищаемой информации. Рассмотрены различные методы социальной инженерии.

Ключевые слова: *социальная инженерия; конфиденциальная информация; информационная безопасность.*

METHODS OF SOCIAL ENGINEERING AS A WAY TO ACCESS INFORMATION OF LIMITED ACCESS

Kizryakova Anastassiya, Solodovnikov Vladislav
St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverksky pr., 49
e-mails: anastasia.kiz6@gmail.com, solsaturate@gmail.com

Abstract. The paper is devoted to social engineering as a way of access to protected information. Various methods of social engineering are considered.

Keywords: *social engineering; confidential information; information security.*

Социальная инженерия является одним из наиболее результативных способов для злоумышленника получить доступ к конфиденциальной информации. Тем не менее, это не всегда учитывается при создании систем защиты информации.

Социальная инженерия – это метод получения незаконного доступа к информации или средствам хранения информации без использования технических средств. Данный метод основан на использовании человеческого фактора, эмоций и является достаточно результативным для злоумышленника.

Все техники применения социальной инженерии основаны на действиях после принятия решений людьми.

Претекстинг представляет собой набор действий, как правило, отработанных по заранее придуманному сценарию. В результате атаки жертва должна сделать определенные действия/

Обратная социальная инженерия – социально-инженерная атака, в которой атакующий создает ситуацию, где жертва сталкивается с проблемой, и просит атакующего о помощи.

Фишинг – техника интернет-мошенничества, при котором злоумышленник получает нужные ему данные. Самая распространённая фишинговая атака: злоумышленник рассылает письма на электронную почту, которые выглядят как официальные письма от банка или платежной системы. В письме находятся форма для ввода персональных данных, либо ссылка на сайт с такой формой.

Квид про кво является техникой, при которой злоумышленник, применяя свое актерское мастерство, представляется сотрудником технической поддержки и сообщает о возникновении технических неполадок или проблем. В ходе разговора атакующий желает получить контроль над компьютером жертвы.

Плечевой серфинг включает в себя сбор личной, конфиденциальной информации путем наблюдения за жертвой через плечо.

Защита от социальной инженерии обязательно должна быть учтена в пользовательском интерфейсе информационной системы. Пользовательский интерфейс должен быть таким, чтобы минимизировать количество ошибок пользователя в результате воздействия на него социальной инженерии[3].

Проанализировав различные методы доступа к конфиденциальной информации при помощи социальной инженерии, можно сделать вывод о том, что все способы защиты информации в организации не являются гарантом обеспечения полной защиты информации, когда присутствует человеческий фактор.

СПИСОК ЛИТЕРАТУРЫ

7. Кевин Митник и Уильям Саймон Искусство обмана 2001 г.
8. Википедия: сайт. - URL: https://ru.wikipedia.org/wiki/Социальная_инженерия
9. Попов А.А. Эргономика пользовательских интерфейсов в информационных системах: учебное пособие / А.А. Попов. М.: РУСАЙНС, 2016. 312с.

УДК 004.056.53

ПРИМЕНЕНИЕ НОВЫХ МОДЕЛЕЙ ВИЗУАЛИЗАЦИИ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРИНИМАЕМЫХ ПОЛЬЗОВАТЕЛЕМ СИСТЕМЫ РЕШЕНИЙ

Коломеец Максим Вадимович[1,2], Чечулин Андрей Алексеевич[1,2]
[1] Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14-я линия В.О., 39
e-mails: chechulin@comsec.spb.ru, kolomeec@comsec.spb.ru

Аннотация. В работе рассматриваются новые модели визуализации систем информационной безопасности, которые позволяют повысить скорость и качество принимаемым оператором решений при визуальной аналитике. Предложена концепция соотношения информативности изображения и эффективности его восприятия в контексте визуального анализа. Предложен перечень графических моделей и примеры их использования в различных областях защиты информации.

Ключевые слова: *визуальная аналитика; информационная безопасность; визуализация данных; модели визуализации.*

APPLICATION OF NEW VISUALIZATION MODELS TO IMPROVE THE EFFECTIVENESS OF USER-MADE SOLUTIONS

Kolomeec Maxim [1,2], ChechulinAndrey [1,2]
[1] ITMO University, Russia, St. Petersburg
[2]St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Russia, St. Petersburg, 14 Liniya,39
e-mails: chechulin@comsec.spb.ru, kolomeec@comsec.spb.ru

Abstract. The paper describes new visualization models for information security systems that allow to increase the speed and quality of decisions made by an operator in visual analytics. The concept of the ratio of the informativity and the effectiveness in the context of visual analysis is proposed. A list of visualization models and examples of their application in various areas of information security is described.

Keywords: *visual analytics; information security; data visualization; visualization model.*

Визуализация данных играет важную роль в обеспечении информационной безопасности. С ее помощью отображают состояние систем и в том числе визуализируют критически важные процессы, нарушение которых может привести к падению экономических показателей, разрушению инфраструктуры или рискам для здоровья и жизни населения. Отслеживать киберугрозы и принимать контрмеры для защиты, специалистам по безопасности помогают системы визуализации, которые вместе с системами защиты формируют комплекс поддержки и принятия решений [1].

Использование визуальной аналитики в системах информационной безопасности обусловлено сразу несколькими факторами. Во-первых, автоматизированные системы плохо справляются с анализом гетерогенных или сильно зашумленных данных. Во-вторых, экспертное решение позволяет лучше раскрыть проблему чем автоматизированный анализ, а использование визуализации позволяет производить экспертное оценивание за приемлемое время.

В-третьих, в информационной безопасности намного больше случаев (в сравнении с другими областями), когда решение принципиально должно приниматься человеком, который будет нести за него ответственность. При этом, эффективность визуальной аналитики в таких системах зависит от выбора используемых моделей визуализации.

Принцип соотношения информативности и эффективности. Каждая модель визуализации обладает двумя свойствами [2] которые влияют на выбор модели при определённом наборе данных: (1) свойство информативности данных, которое выражается в количестве и типовом разнообразии отображаемых метрик; (2) свойство эффективности восприятия информации, которое выражается в скорости и точности интерпретации изображения пользователем. Правильное соотношение

информативности и эффективности в модели визуализации дает лучший результат при визуальном анализе.

На практике информативность выражается возможностью отображения большого количества метрик различных типов, а эффективность выражается скоростью и точностью интерпретации метрик. Очевидно, что чем больше метрик способна отобразить модель визуализации, тем выше ее информативность и ниже эффективность. Для того, чтобы обеспечить необходимый уровень эффективности и достаточный уровень информативности, необходимо выбрать подходящую модель визуализации, которая в силу своих особенностей способна для определённого набора данных отобразить большое количество метрик без потерь эффективности восприятия.

Модели визуализации. Наиболее простая классификация моделей визуализации, это деление моделей на связанные и не связанные [3].

Большинство моделей, такие как графики, параллельные координаты, трилинейные координаты, розы ветров и прочие не способны отображать связанные структуры. Для визуализации связанных структур чаще всего используются Графы, Матрицы и Карты Деревьев. Как правило, для анализа топологий используются графы, для визуализации метрик связей используются матрицы, а карты деревьев используются для визуализации метрик объектов.

Для анализа карт можно использовать модель диаграммы Вороного [4]. Например, диаграммы Вороного можно применять для анализа перемещения человека по сигналу его сотового телефона. Путем эксплуатации уязвимости SS7 [5] можно получить номер базовой станции, к которой подключен телефон. Сформировав Диаграмму Вороного на основе координат базовых станций, можно узнать область, в которой человек находится.

В оценке рисков при анализе киберфизической безопасности помещений можно использовать Карты Вороного. Рассмотрим пример мониторинга поведения сотрудника. Для данного примера используются данные о передвижении, которые основываются на открытии дверей смарт-картой, привязанной к сотруднику. Чем дольше сотрудник находился в комнате, тем более непрозрачной становится ячейка. Размер ячейки основан на ценности активов. А связь между ячейками соответствует дверям между помещениями.

В оценке рисков [3] при анализе состояния компьютерных сетей можно использовать совмещенные модели. На рисунке 3 хосты сети изображены в виде глифов на главной диагонали матрицы, связи как глифы выше и ниже главной диагонали. Глиф хоста состоит их четырех частей (критичность, вероятность компрометации, риск и количество уязвимостей). Глиф связи состоит их двух частей (критичность и вероятность перехода).

В виде графа отображен маршрут злоумышленника (внешняя сеть -> маршрутизатор -> файрвол -> маршрутизатор -> база данных). Численные параметры нормализованы от нуля до единицы и представлены соответственным оттенком цвета.

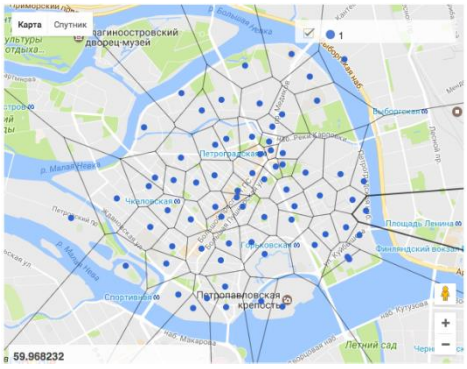


Рисунок 1 – Диаграмма Вороного на основе координат базовых станций оператора «Мегафон» на Петроградском острове

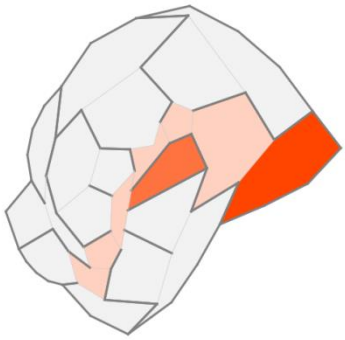


Рисунок 2 – Анализ рисков киберфизической безопасности на основе Карты Вороного

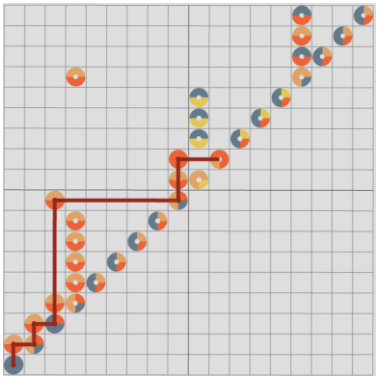


Рисунок 3 – Маршрут атакующего в виде графа, наложенного на матрицу с глифами

Заключение. В работе рассмотрены новые модели визуализации такие как диаграмма Вороного, карты Вороного и совмещенная модель матрицы и глифов. Приведены примеры использования моделей в различных областях визуальной аналитики для обеспечения информационной безопасности. Предложена концепция соотношения информативности изображения и эффективности его восприятия. Также в работе приведен перечень наиболее распространенных моделей визуализации и приведена их классификация. Работа выполнена при финансовой поддержке РФФИ (проект 15-07-07451) и при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007 в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Novikova E., Kotenko I. Analytical Visualization Techniques for Security Information and Event Management // Proceedings of the 21th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013). Belfast, Northern Ireland, UK. 27th February – 1st March 2013. Los Alamitos, California. IEEE Computer Society. 2013. P.519-525.
2. Коломеец М. В., Чечулин А. А., Котенко И. В. Методика визуализации топологии компьютерной сети для мониторинга безопасности //Известия высших учебных заведений. Приборостроение. – 2016. – Т. 59. – №. 10. С. 807-812.
3. KolomeecM.,Gonzalez-Granadillo G., Doynikova E., Chechulin A., Kotenko I., Debar H. Choosing Models for Security Metrics Visualization //International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. – Springer, Cham, 2017. – P. 75-87.
4. Kolomeets M., Chechulin A., Kotenko I. Visualization Model for Monitoring of Computer Networks Security Based on the Analogue of Voronoi Diagrams //International Conference on Availability, Reliability, and Security. – Springer International Publishing, 2016. – P. 141-157.
5. Positive Technologies SS7 Security Report. URL: https://www.ptsecurity.com/upload/iblock/083/08391102d2bd30c5fe234145877ebcc0.pdf

УДК 004.056

ИДЕНТИФИКАЦИЯАТАКНАБЕСПРОВОДНУЮ СЕНСОРНУЮ СЕТЬ НА ОСНОВЕ АНАЛИЗА ПОВЕДЕНИЯ СЕТИ

Коржук Виктория Михайловна
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mail: vika@cit.ifmo.ru

Аннотация. В данной работе кратко описаны особенности использования беспроводных сенсорных сетей, рассмотрены проблемы информационной безопасности и проблемы защиты информации в беспроводных сенсорных сетях. Приведены наиболее часто встречаемые атаки различных видов. Описан исследуемый метод идентификации атак на беспроводные сенсорные сети и описан дальнейших ход работы над поставленной проблемой.

Ключевые слова: *беспроводная сенсорная сеть; анализ поведения; идентификация атак.*

WIRELESS SENSOR NETWORK ATTACK IDENTIFICATION IN THE BASIS OF NETWORK BEHAVIOUR ANALISIS

Korzhuk Victoria
St. Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University)
Russia, St. Petersburg, Kronverkskiy pr.,49
e-mail: vika@cit.ifmo.ru

Abstract. This paper briefly describes the features of wireless sensor network working; the problems of information security and information protection in wireless sensor networks are shown. The most common information security attacks of various types are described. The researched method of identification of attacks on wireless sensor networks is specified and the further course of work on the posed problem is posed.

Keywords: *wireless sensor network; behaviour analisis; attack identification.*

Беспроводные сенсорные сети получают все более широкое распространение. На основе таких сетей построены различные системы мониторинга (загрязнение окружающей среды, военная область, медицина) и управления (умное производство «Индустрия 4.0», умные дома). Поскольку информация, циркулирующая внутри таких сетей, становится более ценной, необходимо обеспечивать конфиденциальность, целостность и доступность информации внутри сети и при обработке на серверах.

Вследствие того, что информация передается по открытым каналам связи, а сами устройства не отличаются технологической сложностью (некоторые устройства представляют собой плату с выведенным датчиком, защищаемую от физических воздействий пластиковым корпусом), для злоумышленника существуют возможности воздействия на такие сети. Пассивные атаки, такие как прослушивание сети и перехват сообщений, не влияют на работоспособность и сети и могут повлиять на конфиденциальность передаваемой информации только в том случае, если злоумышленник имеет четкое представление о структуре и назначении сети и понимает, данные какого формата передает устройство.

Активные атаки (например, атаки маршрутизации) имеют гораздо более разрушительное воздействие и могут привести к выходу из строя как одного или нескольких устройств, так и всей сети в целом. В зависимости от вида объекта, на котором установлена и функционирует такая сеть, выход из строя даже одного устройства может быть критичен.

Однако, производителем и системный администратором установлены настройки, в соответствии с которыми должна функционировать такая сеть. Такими настройками является скорость передачи данных, количество переданных пакетов, количество переданных кадров, среднее время работы устройств, время перехода в и из спящего режима и т.д. Отклонение от нормы поведения может свидетельствовать о проводимой/проведенной атаке.

В соответствии с этим, целью работы является разработка метода идентификации атак на беспроводную сенсорную сеть на основе анализа поведения сети. В рамках работы было разработано признаковое пространство, содержащее различные типы признаков, в т.ч. признаки-соотношения, необходимые в случаях, когда признаки по отдельности не имеют высокой информативности, однако при отношении признаков друг к другу проявляют достаточную степень информативности. С помощью математической оценки информативности был выделен набор признаков, позволяющих в короткое время идентифицировать атаки типа «Червоточина», «Сибилла», «Флуд» и др.

В дальнейшем планируется использовать машинное обучение для разработки системы мониторинга информационной безопасности беспроводной сенсорной сети, выбрать наиболее подходящие методы обработки информации и представить методику идентификации атак на беспроводные сенсорные сети.

СПИСОК ЛИТЕРАТУРЫ

1. Novikova E., Kotenko I. Analytical Visualization Techniques for Security Information and Event Management // Proceedings of the 21th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013). Belfast, Northern Ireland, UK. 27th February – 1st March 2013. Los Alamitos, California. IEEE Computer Society. 2013. P.519-525.

УДК 004.056.53

АНАЛИЗ ЗАЩИЩЕННОСТИ ERP-СИСТЕМ. ОБЩИЙ ПОДХОД К АНАЛИЗУ

Кривдюк Надежда Михайловна
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mail: krivduk.nadezhda@gmail.com

Аннотация. Рассмотрены наиболее известные проблемы безопасности ERP-систем, ранжированные по степени важности и влияния на корпоративные приложения в целом. В ходе исследования был предложен подход анализа защищенности корпоративных приложений, покрывающие все критичные области любой ERP-системы.

Ключевые слова: *ERP-системы; анализ защищенности; Top-9 ERP Issues; настройки безопасности; критичность проблем; EAS-SEC.*

ANALYSIS OF ERP-SYSTEMS SECURITY. GENERAL APPROACH TO ANALYSIS

Krivdyuk Nadezhda
St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverksky pr., 49
e-mail: krivduk.nadezhda@gmail.com

Abstract. The most known security problems of ERP-systemsare considered, ranged by the degree of importance and influence on corporate applications in general. In the course of the study, an approach was proposed to analyze the security of enterprise applications, covering all critical areas of any ERP-system.

Keywords: *ERP-systems; security analysis; Top-9 ERP Issues; security settings; criticality of problems; EAS-SEC.*

Современное общество характеризуется стремительным развитием новейших информационных технологий, где постоянно циркулирует информация. Вместе с чем значительно возрастают угрозы безопасности информации, что может привести к нарушению непрерывности бизнеса. В связи с этим очевидна необходимость обеспечения безопасности организаций.

В крупных компаниях и не только вся критичная информация хранится и обрабатывается в корпоративных приложениях и системах: веб-приложения, СУБД, системах управления ресурсами предприятия (ERP-системы) и других. Такая информация может содержать финансовые данные, коммерческую тайну, персональные данные и иную специфическую информацию, которой заинтересованы злоумышленники[1].

Объектом исследования выбраны ERP-системы, так как в них обрабатываются наиболее критичная информация. В ходе исследования проанализированы существующие рекомендации по безопасности от Oracle, ISACA[2], OWASP[3], PCIDSS и BIZEC и других, а также доклады крупных конференций по информационной безопасности. Задачей исследования стояло захватить вниманием

как можно больше проблемных областей в ERP-системах, для которых необходимо проведение анализа защищенности.

В процессе исследования были выбраны и описаны самые критичные проблемы, оказывающие негативное воздействие на системы, и определить приоритеты решения данных проблем. Были определены области, внутри которых необходимо осуществить безопасность. При этом, важно было выделить те области, которые являются наиболее распространёнными в Корпоративных Приложениях. Кроме высокой частоты обнаружения этих проблем, необходимо было понять еще несколько фактов о каждой из них. В результате среди многообразия проблем ERP-систем были выбраны девять самых критичных, ранжированы по степени важности и влияния на корпоративные приложения в целом, и безопасность EAS в частности. Для этого было утверждены критерии: уровень авторотационного доступа, критичность проблемы, сложность использования проблемы и частота встречаемости проблемы.

В результате анализа появился окончательный вариант ранжированного по критичности списка девяти наиболее распространенных проблем ERP-систем Top-9 ERP Issues:

1. Недостатки управления обновлениями.
2. Учетные записи по умолчанию для доступа к приложению.
3. Дополнительный функционал.
4. Открытые удаленные интерфейсы управления.
5. Небезопасные настройки.
6. Незашифрованные соединения.
7. Контроль доступа и SOD конфликты.
8. Небезопасные доверенные соединения.
9. Протоколирование событий безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. «Система планирования ресурсов предприятий ERP», RBC group – Решения по управлению предприятиями на основе систем ERP и BI, [Электронный ресурс], URL: http://www.rbcgrp.com/erp-planing.html, режим доступа: свободный, дата обращения: 19.09.2017.
2. Information Technology - Information Security – Information Assurance | ISACA [Электронныйресурс] / Режимдоступа: https://www.isaca.org (19.09.2017)
3. OWASP, Top 10 Application Security Risks [Электронныйресурс] / Режимдоступа: https://www.owasp.org/index.php/Top_10_2017-A2-Broken_Authentication_and_Session_Management (19.09.2017)

УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАЩИЩЕННОСТИ ОСУЩЕСТВЛЕНИЯ ФИНАНСОВЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

Курышева Алена Андреевна, Ганчикова Юлия Сергеевна
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: kurysheva.al@yandex.ru, yul7494582@yandex.ru

Аннотация. Работа посвящена сравнительному анализу защищенности финансовых операций с использованием электронных платежных систем. Рассмотрены уровни защищенности нескольких платежных систем предназначенных для оплаты товаров и услуг в сети Интернет.

Ключевые слова: *финансовая безопасность; платежные системы; транзакции; защита; 3D-secure.*

COMPARATIVE ANALYSIS OF FINANCIAL TRANSACTIONS SECURITY USING ELECTRONIC PAYMENT SYSTEMS

Kurysheva Alena, Ganchikova Yulia
St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverksky pr., 49
e-mails: kurysheva.al@yandex.ru, yul7494582@yandex.ru

Abstract. The article presents analysis of security transactions using electronic payment systems. The article considered levels of security of several payment systems designed to pay for goods and services on the Internet.

Keywords: *financial security; payment system; transactions; security; 3d-secure.*

На сегодняшний день электронные платежные системы используются миллионами пользователей ежедневно. Сохранность персональных данных и денежных средств зависит от безопасности проведения транзакций в платежных системах.

Рассматриваемые электронные платежные системы предназначены для упрощения проведения финансовых операций при помощи сети Интернет. Для сравнительного анализа использованы следующие платежные сервисы: «QIWI», «WebMoney», «PayPal», «Яндекс.Деньги». Проведено сравнение электронных платежных систем по следующим критериям: шифрование, аутентификация, идентификация, дополнительное подтверждение операции, дополнительная защита.

Сравнительный анализ позволяет сделать вывод, что каждая рассмотренная электронная платежная система имеет несколько уровней защиты. Процесс подтверждения операций у каждой из платежных систем имеет свой алгоритм и от этого напрямую зависит безопасность транзакций. Часть рассмотренных платежных систем имеет более низкий уровень безопасности. Для повышения уровня следует уделить более пристальное внимание аутентификации, идентификации и алгоритму подтверждения финансовых операций.

СПИСОК ЛИТЕРАТУРЫ

1. Никонец О. Е., Гринь И. А., Марченко А. В. Бесконтактные платежи: история возникновения и безопасность // Научно-методический электронный журнал «Концепт». – 2016. – Т. 15. – С. 2726–2730. – URL: http://e-koncept.ru/2016/96466.htm (дата обращения: 16.09.2017).
2. О национальной платежной системе [Электронный ресурс] : федер. закон Рос. Федерации от 27 июня 2011 г. №161-ФЗ: принят Гос. Думой 14 июня 2011 г. : одобр. Советом Федерации 22 июня 2011 г. (ред. от 18.07.2017). Доступ из справ.-правовой системы «КонсультантПлюс».

УДК 004.056

МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ КЕСМ-СИСТЕМАМ

Лейфер Анастасия Александровна
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mail: vika@cit.ifmo.ru

Аннотация. Безопасность электронных документов – важная проблема для организаций. Выполнение требований безопасности позволяет организациям эффективно функционировать и сохранять их коммерческие преимущества.Рассмотрены системы по управлению корпоративным контентом, а также их инструментарий, применимый для защиты информации. В работе редставлены принципы формирования требований безопасности к системам данного класса, а также общая модель таких требований.

Ключевые слова: *управление корпоративным контентом; электронный документооборот; требования безопасности; модель.*

METHODOLOGY FOR FORMING SECURITY REQUIREMENTS TO ECM SYSTEMS

Leyfer Anastasiya
ITMO University
Russia, St. Petersburg, Kronverksky pr.,49
e-mail: vika@cit.ifmo.ru

Abstract. Electronic documents security is important problem for organization. Implementation of security requirements allows organization to work effectively and keep their commercial advantages. The article deals with enterprise content management systems, and its functions that can be used for information security purposes. The paper presents princes of creating security requirements for ECM systems and common model of requirements.

Keywords: *enterprise content management; electronic document management; security requirements; model.*

Security is a process, not a product
(Bruce Schneier)

Безопасность - это процесс, а не продукт
(Брюс Шнайер)

Информация – основной актив современной организации. Количество обрабатываемых данных растет каждый день, а вместе с ними и число угроз безопасности. Угрозы информационной безопасности реализуются в результате удаленных атак, происков конкурентов, действий внутренних нарушителей, физических и других воздействий. Несмотря на ажиотаж вокруг хакерских атак,

зачастую опасность таится внутри организации, а многие вопросы безопасности, требуют, в первую очередь, внимания руководства.

Электронный документ – важный инструмент, сопровождающий производственную или иную деятельность организации. Предприятия должны прилагать достаточное количество усилий для обеспечения защищенности документации с целью сохранения коммерческих преимуществ. Кроме того, для успешного функционирования организации процессы и результаты защиты документов должны соответствовать законодательству и другим отраслевым нормативным документам. Меры по информационной безопасности часто принимаются уж после инцидентов. Активная деятельность по защите электронных документов начинается уже после того, как произошла утечка конфиденциальной безопасности или были реализованы другие угрозы информационной безопасности. Поэтому существует необходимость формирования модели и методологии требований безопасности на начальном этапе создания информационной системы.

К основным классам систем по управлению электронными документами относятся системы электронного документооборота (далее - СЭД) и системы по управлению корпоративным контентом (далее – ECM, от англ. Enterprise content management). Некоторые эксперты отождествляют понятия СЭД и ECM, однако при тщательном изучении становятся очевидны различия между этими классами систем. Сложность определения различий между ECM и СЭД обусловлена отсутствием стандартизации данного класса систем в России и неоднозначности интерпретации зарубежной терминологии [1]. Некоторые исследователи считают ECM западным аналогом СЭД, другие – системой с идентичным функционалом. В то время как ECM обладает рядом существенных отличий, как фундаментальных, так и прикладных. СЭД – это, в первую очередь, инструмент решения насущных проблем, ECM – методология и концепция, включающая в себя больше, чем решение прикладных задач. В рамках данного исследования два класса систем будут разделены и рассмотрены только ECM. Однако системы во многом схожи, поэтому большинство результатов может быть применено и к СЭД.

Таким образом, целью данного исследования является формирование обобщенной модели требований безопасности к ECM-системам. Для достижения цели поставлены следующие задачи:

1. Рассмотреть общие функциональные возможности ECM.
2. Рассмотреть инструментарий ECM, применимый для защиты информации.
3. Определить место требований безопасности в структуре общих требований.

Управление корпоративным контентом - управление цифровыми документами и другими типами контента, а также их хранение, обработка и доставка в рамках организации [2]. Под корпоративным контентом понимается как структурированная, так и не структурированная информация, используемая в деятельности предприятия: бумажная и электронная документация, электронные таблицы, презентации, почтовые сообщения, видео, фото. ECM-система – программное обеспечение для управления корпоративным контентом. Далее будет рассмотрен документ как основной тип хранящегося контента. Основными функциями ECM являются хранение и поиск документов. Документы хранятся в иерархической структуре папок, доступ к которой определяется политиками безопасности. Для поиска возможно два варианта: контекстный и атрибутивный. Контекстный поиск осуществляется по ключевым словам в содержательной части документов, атрибутивный – среди присвоенных документу атрибутов. Другие прикладные функции ECM: организация жизненного цикла документов, аудит действий пользователей, версионность, автоматизация документоориентированных бизнес-процессов.

Работа пользователя с ECM начинается с авторизации. Механизм аутентификации является стандартным, как и в других корпоративных ИС. После авторизации пользователю становятся доступны документы, к которым у него есть права доступа. Доступ к хранящимся документам определяется политиками безопасности, которые представляют собой совокупность ролей (читатель, редактор, владелец и др.) и назначенных на роли разрешений (открыть, сохранить, добавить новую версию и др.). Ролевые политики современных предприятий отличаются сложностью, которая, в свою очередь, обуславливается многообразием хранимого контента и видов защищаемой информации. Политики безопасности должны быть гибкими и основываться на организационной структуре предприятия (линейной, функциональной, матричной, дивизионной или смешанной). Кроме того, ролевая модель должна быть задокументирована и утверждена руководством. Для контроля действий пользователей с документами и папками, к которым они имеют доступ, используется протоколирование. Протоколирование представляет собой процесс сбора данных о системных событиях и действиях пользователя. Аудит, как результат анализа протоколирования, делает возможным расследование инцидентов. Срок хранения результатов должен составлять величину, достаточную для расследования случаев утечки защищаемой информации. Ролевые политики и протоколирование используются, в первую очередь, для предотвращения и нейтрализации внутренних угроз.

В ECM контент хранится в зашифрованном виде, при этом сами документы могут храниться в файловой системе, а их атрибутивные карточки – в базе данных.

Таким образом, если злоумышленник получает доступ к одному из ресурсов, он по-прежнему не обладает полной информацией. Шифрование также применяется в ЭЦП, однако подпись обычно не включена в стандартные функции ECM и реализуется отдельным программным средством. ЭЦП является важным элементом электронного документооборота, придает ему юридическую значимость. Она может быть использована как внутри организации, так и при обмене информацией с внешними субъектами. Тип подписи и технология реализации обуславливаются потребностями конкретной организации.

С архитектурной точки зрения безопасность обеспечивают механизмы кластеризации и резервного копирования. Кластеризация необходима для равномерного распределения нагрузки на систему, что является важным для больших распределенных архитектур. Резервирование позволяет восстановить данные в случае восстановления сбоев или атак на ресурсы.

Таким образом, мы рассмотрели следующие инструменты защиты информации:

- ролевые политики доступа;
- протоколирование и аудит;
- шифрование хранящегося контента;
- электронная цифровая подписи;
- кластеризация и резервное копирование.

Функции рассмотрены в общем виде, однако каждая из них является гибкой и при проектировании должна быть определена более точно. Это позволит, во-первых, достичь наиболее эффективного режима работы, во-вторых, сделать затраты минимально необходимыми. Требования к рассмотренным функциям должны быть соотнесены с требованиями безопасности к системе в целом [3].

Требования к внедряемой системе можно разделить на системные требования и пользовательские. В число системных требований входят требования к доступности системы. Система может функционировать в различных режимах, например, 24 часа 7 дней в неделю или 9 часов 5 дней в неделю, в зависимости от критичности системы. Выбранный режим работы должен быть обеспечен вычислительными мощностями. Другая характеристика системы - время восстановления данных после сбоя. Восстановление данных происходит благодаря использованию резервных станций, системные характеристики которых должны быть результатом предварительного анализа. Организация должна понимать, во сколько ей обойдется минута простоя. Для выявления общих пользовательских потребностей часто используются пользовательские сценарии использования. Они позволяют понять поведение пользователя и сделать взаимодействие пользователя с системой наиболее удобным, безопасным и эффективным. Для формирования частных требований безопасности могут быть использованы сценарии нарушителей, также с целью моделирования поведения. Однако тут есть отличие от пользовательских сценариев использования: целью является не воспроизведение оптимального взаимодействия человека и системы, а предотвращение моделируемого поведения и, непосредственно, реализации угрозы. Модель нарушителя также может быть представлена и другими, более формальными методами.

Можно выделить несколько этапов создания ИС: обследование объекта, сбор требований к системе, проектирование и внедрение. Для наиболее эффективного функционирования системы и минимизации инцидентов требования должны быть заложены на начальных этапах создания ИС, а не в процессе непосредственно внедрения или реализации. Требования безопасности к системе должны быть рассмотрены в контексте общих системных требований и не могут быть от них отделены. Кроме того, они должны быть формализованы и задокументированы. Работа служб безопасности в ECM должна быть согласована с другими службами и системами ИТ-инфраструктуры предприятия.

ECM-системы, как и любых другие корпоративные системы, помимо своей прикладной функции должны выполнять функцию поддержания безопасности. Понимание важности вопросов безопасности постепенно приходит к организациям, однако за пониманием не всегда следует реализация. В данной работе рассмотрены общие функции и требования безопасности к ECM, выполнение которых позволит обеспечить безопасность бизнес-критичного контента предприятия. Полученная модель является основой для формирования частных моделей по сферам деятельности (финансовая, промышленная сферы, здравоохранение, государственный сектор и др.), и типам хранимой информации (коммерческая тайна, служебная тайна, профессиональная тайна, персональные данные и др.)

СПИСОК ЛИТЕРАТУРЫ

1. Стандарт MoReq-2 «Типовые требования по управлению электронными официальными документами»
2. Ассоциация по вопросам Управления Информацией и Изображениями (Association for Information and Image Management, AIIM) [Электронный ресурс] – URL: http://www.aiim.org/
3. Системы электронного документооборота, ECM-системы: учебное пособие / Филяк П.Ю., 2014. – 108 с.
1. Маглинец, Юрий Анатольевич. Анализ требований к автоматизированным информационным системам: учебное пособие / Ю. А. Маглинец. - Москва: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2014. -200 с

УДК 004.93:57.087.1

СИСТЕМА СБОРА И АНАЛИЗА ДАННЫХ ДЛЯ ИССЛЕДОВАНИЯ УНИКАЛЬНОСТИ ПОВЕДЕНЧЕСКИХ ПРИЗНАКОВ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ УСТРОЙСТВ

Лейфер Кирилл Ильич
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mail: leyfer.kirill@gmail.com

Аннотация. Данная работа является очередным этапом исследования поведенческих признаков и динамических биометрических характеристик пользователей мобильных устройств с целью последующего построения метода идентификации (аутентификации), основанного на этих признаках. В рамках данной работы построена и протестирована новая система сбора данных, разработана новая методика анализа полученных данных и проведён предварительный анализ небольшого набора собранной информации.

Ключевые слова: *биометрия; поведенческие признаки; мобильные устройства; идентификация; аутентификация.*

SYSTEM OF DATA COLLECTION AND ANALYSIS FOR THE STUDY OF THE UNIQUE BEHAVIOR SIGNS OF MOBILE DEVICEUSERS

Leyfer Kirill
ITMO University
Russian Federation, St. Petersburg, Kronverksky pr., 49
e-mail: leyfer.kirill@gmail.com

Abstract. This work is the next stage in the study of behavioral characteristics and dynamic biometric characteristics of mobile device users with an intention to construct a method of identification (authentication) based on these characteristics. In this work a new data collection system was constructed and tested, a new technique for analyzing the data was developed, and a preliminary analysis of a small set of collected information was carried out.

Keywords: *biometrics; behavioral signs; mobile devices; identification; authentication.*

Смартфон можно назвать самым личным электронным устройством в жизни современного человека. Пользователи практически не расстаются со смартфонами и доверяют им множество ценной информации. К тому же смартфон воспринимается не как полноценный компьютер (коим, безусловно, является), а, скорее, как телефон, вследствие чего бдительность пользователя снижается. В таких условиях задача защиты пользовательской информации стоит как никогда остро.

В последнее время наблюдается тенденция к внедрению в смартфоны средств биометрической аутентификации, которые, при наличии определённых преимуществ (простота использования, надёжность и так далее), подвержены и недостаткам (возможность скопировать аутентификатор, либо воспользоваться им против воли владельца устройства). Для увеличения надёжности аутентификации имеет смысл добавить ещё один фактор: поведенческий. При всех своих недостатках этот фактор, используясь совместно с остальными, способен повысить надёжность аутентификации в целом.

Поведенческий фактор хорошо подходит для внедрения в смартфоны: эти устройства оснащены большим количеством сенсоров, точность которых может зафиксировать некоторые уникальные для каждого пользователя характеристики или паттерны поведения.

До построения многофакторной системы аутентификации с использованием поведенческого фактора следует найти оптимальное признаковое пространство, собрать данные, соответствующие выбранным признакам и провести исследование собранных данных, оценивая применимость выбранного пространства признаков для построения системы аутентификации.

В конце 2015 г. проводился сбор данных среди 20 тестовых пользователей. Данные представляли собой жесты, которые пользователи вводили на сенсорных экранах своих устройств. Исследование полученных данных легло в основу работы [1] и показало, что из жестов можно извлечь характеристики, уникальные для пользователей, но эта уникальность сама по себе недостаточно высока.

Возникла необходимость расширить признаковое пространство, для чего было проведено исследование, которое легло в основу работы [2]. По результатам исследования было предложено расширить пространство признаков информацией о текущей активности, в которой работает пользователь, и показаниями акселерометра и гироскопа, встроенных в смартфон.

В рамках данной работы была усовершенствована техническая часть. Главный недостаток предыдущей версии – строго ограниченный набор поддерживаемых устройств (11 различных моделей android-смартфонов). Это ограничение было вызвано примитивным методом преобразования данных, поступающих из драйвера сенсорного экрана. Для каждого устройства

приходилось вручную находить параметры, при которых преобразование выполнялось правильно. Новая версия использует модифицированный код системы ввода из AOSP (Android Open Source Project - проект Android с открытым исходным кодом), поэтому работает практически на всех android-устройствах, автоматически подбирая верные параметры и поддерживая несколько протоколов, по которым работают драйвера сенсорных экранов.

Так же старая версия требовала прав root для нормальной работы, что тоже ограничивало количество поддерживаемых устройств. Такое требование было вызвано ограниченными правами доступа к символьному устройству сенсорного экрана. Новая версия способна обходиться без root-прав. Достичь этого удалось благодаря внедрению нескольких способов запуска сбора данных:

– Запуск с использованием root-прав
– Ручной запуск от имени пользователя shell (через отладочную консоль Android-устройства)
– Автоматический запуск от пользователя root через уязвимость CVE 2016-5195 (подробно описан в [3])

Помимо этого, в [2] техническая часть была расширена системой сбора данных с гироскопа и акселерометра, а также системой мониторинга запущенных активностей.

Таким образом, техническая часть по-прежнему способна отправлять все собранные данные на сервер и работать в фоновом режиме. Сервер так же сохраняет принятые данные в БД для последующего анализа.

В [1] проводился анализ распределения серии жестов по их длине и продолжительности, и полученные векторы для каждого пользователя сравнивались между собой. Для сравнения применялась серия бинарных классификаторов, предварительно обученных на пользовательских данных, полученных за предыдущий период. В данной классификации за неимением нужных данных не учитывалось, в какой активности вёл работу пользователь.

С расширением пространства признаков был выбран следующий способ анализа: сравнивая активности и жесты по меткам времени, можно для каждого жеста найти активность, в которой он был введён. Зная эту информацию, можно построить распределение жестов, введённых в одной и той же активности, по некоторым признакам. Сравнивая такие жесты между разными пользователями, можно легко выделить уникальные для пользователей признаки этих жестов.

Эту систему можно улучшать по мере получения новых данных. Обнаружив схожие паттерны взаимодействия с различными активностями, можно сами активности так же разбить на классы, и сравнивать жесты различных пользователей, введённые не в одной и той же активности, а в одном и том же их классе.

Сами активности так же представляют отличный материал для исследования: обладая информацией о том, какая активность была запущена в каждый момент времени, можно построить различные паттерны поведения пользователя. Самым простым примером будет распределение использования активностей по продолжительности, распределение вероятности запуска активности в зависимости от времени суток, дня недели и так далее. Более интересный пример — построение цепи Маркова на основе вероятностей перехода пользователя между активностями. Сравнение получаемой на устройстве истории перемещения пользователя по активностям и сравнение этой истории с эталонной цепью Маркова позволит сразу же вычислять вероятность того, что именно владелец устройства пользуется им в данный момент.

Наличие данных с акселерометра и гироскопа в теории позволит строить жесты в пяти измерениях: координаты жестов на экране, а также положение смартфона в пространстве во время ввода жеста (его поворот относительно осей X, Y и Z). Такое расширение пространства признаков призвано повысить точность классификации. Однако на практике возникает проблема в сопоставлении жестов с событиями датчиков по времени, так как данные с датчиков поступают с некоторой задержкой относительно событий ввода, причём величина задержки неизвестна и уникальна для каждого устройства. Поиск путей решения этой проблемы так же является интересной задачей.

Заключение. В данной работе была улучшена техническая часть проекта, проведён её тестовый запуск и отладка, в процессе которых был получен небольшой набор тестовых данных. Этот набор позволил разработать новые способы анализа данных, недоступные для набора данных, полученного с помощью старой версии технической части.

СПИСОК ЛИТЕРАТУРЫ

1. Lefyer K., Spivak A. Method of Person Identification Based on Biometric Characteristics of Touch Screen Gestures // Proceedings of the 20th Conference of Open Innovations Association FRUCT - 2017, pp. 222-227
2. Лейфер К.И., Спивак А.И. Определение пространства признаков для идентификации пользователя на мобильных устройствах // Альманах научных работ молодых ученых - 2017. - Т. 4. - С. 33-35

Реализуем тач логгер под Android с помощью CVE-2016–5195 [Электронный ресурс]. URL:

УДК 004.056.53

АНАЛИЗ СУЩЕСТВУЮЩИХ ДАТЧИКОВ ДЛЯ ВЫЯВЛЕНИЯ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

Лисецкая Кристина Валерьевна
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mail: kristinasev62@gmail.com

Анотация.Рассмотрены наиболее эффективные датчики для создания комплексной системы защиты, которые помогают предотвратить несанкционированный доступ к информации. Определены и проанализированы их главные достоинства и недостатки. Описан принцип работы каждого компонента комибинированного датчика.

Ключнвые слова: *системы контроля доступа; датчик; несанкционированный доступ; комбинированный датчик.*

ANALYSIS OF EXISTING SENSORS FOR DETECTING THE ATTEMPTS OF UNAUTHORIZED ACCESS TO PROTECTED INFORMATION

Lisetskaya Kristina
St. Petersburg National Research University Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverksky pr.,49
e-mail: kristinasev62@gmail.com

Abstract. The article deals with the most effective sensors for creating an integrated security system that prevents unauthorized access to information. The main advantages and disadvantages are determined and analyzed. The principle of operation of each component of the combined sensor is described.

Keywords: *access control systems; sensor; unauthorized access; combined sensor.*

На сегодняшний день остро стоит проблема безопасности, а именно, охраны предприятия от несанкционированного доступа к защищаемой информации. Системы контроля доступа прогрессируют и их значимость увеличивается. Нередко на предприятиях используют для надёжной защиты своих данных такие устройства, как датчики. Однако, при выборе необходимо помнить о следующих важных факторах: цена, качество и надёжность.

Основная часть. Рассматриваются датчики, которые чаще всего применяют в системе контроля доступа, их достоинства и недостатки. Проведя сравнительный анализ датчиков, используемых в системе защиты были выбраны наиболее эффективные. Для достижения максимального результата их следует использовать в комплексе, так как каждый извещатель имеет свою уязвимость. Описаны принцип работы каждого составляющего устройства.

В результате проведенного анализа, выявлено, что каждый из датчиков склонен к уязвимостям, поэтому необходимо их использовать в комплексе. Используя комбинированный датчик повысится надёжность всей системы. Данное устройство обеспечит предотвращение нарушения охраняемого периметра, а также несанкционированного доступа к защищаемой информации.

СПИСОК ЛИТЕРАТУРЫ

1. Умные датчики для интеллектуальных систем безопасности. [электронный ресурс], режим доступа: http://www.vashdom.ru/articles/st_16.htm
2. Электротехническая энциклопедия #16.Датчики. [электронный ресурс], режим доступа: http://electrolibrary.info/subscribe/sub_16_datchiki.htm
3. Основные характеристики датчиков. [электронный ресурс], режим доступа: http://studopedia.ru/2_66109_osnovnie-harakteristiki-datchikov.html
4. Датчики охранной сигнализации. [электронный ресурс], режим доступа: http://sec4all.net/datchik.html
5. Извещатели комбинированные и совмещенные. [электронный ресурс], режим доступа: http://specautomatik.ru/index.php/article/211-kombinirovannye

УДК 004.056.53

АНАЛИЗ ВОПРОСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ МЕДИЦИНСКОГО НАЗНАЧЕНИЯ

Лосев Роман Вячеславович, Ручкан Александр Дмитриевич
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mail: roma-2224@ya.ru

Аннотация. В докладе рассмотрены существующие варианты применения беспроводных сенсорных сетей в медицине, проанализирована проблема обеспечения конфиденциальности, целостности и доступности передаваемых данных (особое внимание будет уделено тому, что

информация представляет собой персональные данные пациента), выявлены уязвимости и предложены варианты для их устранения.

Ключевые слова: *беспроводная сенсорная сеть, информационная безопасность.*

THE ANALYSIS OF QUESTIONS OF INFORMATION SECURITY ON THE WIRELESS SENSOR NETWORKS OF MEDICAL ASSIGNMENT

Losev Roman, Ruchkan Alexander
St. Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg,Kronverkskiy pr., 49
e-mail: roma-2224@ya.ru

Abstract. In the report deals with the existing ways of use of wireless sensor networks in medicine, analyses problems of confidentiality, integrity and availability of transferring data (the feature is that the transfrerring information is the client personal data), reveal specific vulnerabilities and offers the ways of eliminations ones.

Keywords: *wireless sensor network, information security.*

В настоящее время беспроводные сенсорные сети получают все более широкое распространение. На основе таких сетей строятся системы экологического мониторинга окружающей среды (в т.ч. контроль уровня загрязнения окружающей среды и распределенный контроль в сельском хозяйстве), системы мониторинга зданий и сооружений, системы контроля производства различной продукции и более глобальные системы, такие как Индустрия 4.0, системы слежения в военной области и медицинского назначения.В современной медицине одной из важнейших проблем является организация процесса наблюдения за показателями физического состояния пациентов (пульс, температура, частота дыхания, кровяное давление, электрокардиограмма, количество сахара в крови), находящихся на лечении в больницах, клиниках или удаленно при минимальном участии медицинского персонала.

По данным, приведенным в работах Бреннана, Липа и др., от 4 до 17% смертельных случаев в больницах США вызваны остановкой сердца. Исследователи поясняют, что около 70% случаев могли бы быть предотвращены при заблаговременном обнаружении ухудшения состояния пациентов. Выявление таких ситуаций возможно при помощи анализа данных, полученных при систематическом наблюдении за определенными показателями состояния организма пациента.

В работе рассмотрены существующие варианты применения беспроводных сенсорных сетей в медицине, проанализирована проблема обеспечения конфиденциальности, целостности и доступности передаваемых данных (особое внимание будет уделено тому, что информация представляет собой персональные данные пациента), выявлены уязвимости и предложены варианты для их устранения.

Решение данной проблемы позволит быстрее и точнее диагностировать заболевания, а также упростит процесс мониторинга пациентов при лечении, в особенности в послеоперационный восстановительный период.

СПИСОК ЛИТЕРАТУРЫ

1. Умные датчики для интеллектуальных систем безопасности. [электронный ресурс], режим доступа: http://www.vashdom.ru/articles/st_16.htm

УДК 004.03

ОБЗОР СУЩЕСТВУЮЩИХ РЕШЕНИЙ СИСТЕМ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лямзина Алиса Григорьевна, Коржук Виктория Михайловна
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: lyamzinaalisa@mail.ru, vika@cit.ifmo.ru

Аннотация. В данной работе кратко описаны особенности использования активного и пассивного мониторинга для управления информационной безопасностью в компании. Приведено описание типовой системы мониторинга информационной безопасности, указаны возможные варианты реализации и составляющие такой системы. Описаны сферы применения систем мониторинга информационной безопасности, выделены особо актуальные области. Указаны дальнейшие планы по развитию данной тематики.

Ключевые слова: *мониторинг информационной безопасности; активный мониторинг; пассивный мониторинг; события информационной безопасности.*

THE REVIEW OF EXISTING DECISIONS OF INFORMATION SAFETY MONITORING SYSTEMS

Lyamzina Alisa, Korzhuk Victoria
St. Petersburg National Research University of Information Technologies,
Mechanics and Optics (ITMO University)
Russia, St. Petersburg, Kronverkskiy pr.,49
e-mails: lyamzinaalisa@mail.ru, vika@cit.ifmo.ru

Abstract. This paper briefly describes the features of using active and passive monitoring in order to manage effectively the information security of a company. A typical information security monitoring system is described; possible implementation options and components of such systems are indicated. Areas of application of information security monitoring systems are described. Especially topical areas are highlighted. Further plans for the development of this subject are posed.

Keywords: *information security; information protection; active monitoring; passive monitoring; information security events; SIEM.*

В наши дни сбор и анализ статистики событий информационной безопасности является одним из важнейших процессов, необходимых для достижения заданного уровня защищенности компании. Активный и пассивный мониторинг состояния системы позволяет обеспечить контроль за состоянием программно-аппаратного комплекса, инвентаризацию ресурсов, управление уязвимостями, контроль соответствия политикам безопасности и происходящих в системе изменений.

Система мониторинга событий информационной безопасности предназначена для автоматизации процесса сбора и анализа информации о регистрируемых событиях безопасности, поступающих из различных источников. В качестве таких источников могут выступать средства защиты информации, общесистемное и прикладное обеспечение, телекоммуникационное обеспечение и др.

Типовая система мониторинга информационной безопасности состоит из следующих компонентов:

1) программно-аппаратный – реализуется на основе продуктов по мониторингу событий безопасности класса SIEM (Security Information and Event Management);

2) нормативный – включает в себя широкий набор документов различного характера, описывающих основные процессы, связанные с выявлением и реагированием на инциденты безопасности;

3) кадровый – подразумевает выделение сотрудников, имеющих или получающих соответствующую квалификацию, ответственных за работу с системой мониторинга информационной безопасности.

В основном, все виды систем мониторинга информационной безопасности объединяет то, что они осуществляют сбор и анализ событий безопасности от разнородных приложений, операционных систем, сетевых устройств, телекоммуникационного оборудования и систем информационной безопасности и т.п. В том числе, такие системы могут быть использованы в наиболее активно развивающихся областях – Умных домах и Индустрии 4.0 («умное производство»), основанных на использовании беспроводных сенсорных сетей.

Особенно актуально применение разрабатываемой системы в области медицины, так как она позволит оперативно реагировать на любые отклонения в работе устройств и сети в целом, что для указанной области обладает критичной важностью в связи с непосредственным отношением к жизни пациентов.

В дальнейшей работе будет проведен анализ сетей такого типа и предпринята попытка разработки модели системы мониторинга информационной безопасности беспроводной сенсорной сети.

СПИСОК ЛИТЕРАТУРЫ

1. Умные датчики для интеллектуальных систем безопасности. [электронный ресурс], режим доступа: http://www.vashdom.ru/articles/st_16.htm

УДК 004.021

ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ МЕТОДА КУСТА СОБЫТИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Наумов Андрей Дмитриевич, Попов Илья Юрьевич
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: adnaumov@corp.ifmo.ru, ilyapopov27@gmail.com

Аннотация. Целью данной работы является исследование применимости метода куста событий в области информационной безопасности. Результатом работы является модель

представления анализируемого процесса на примере транзакции. Такие модели можно применять в различных случаях, связанных с выявлением и анализом нетипичных значений, и в конечном счете прийти к формальной классификации информационных угроз в зависимости от свойств модели.

Ключевые слова: *куст событий; модель; методология; информационная безопасность; угрозы безопасности.*

INVESTIGATION OF THE APPLICABILITY OF THE METHOD OF EVENT BUSH IN THE FIELD OF INFORMATION SECURITY

Naumov Andrey, Popov Ilya
[1] St. Petersburg national research university of information technologies, mechanics and optics (ITMO University)
Russia, St. Petersburg, Kronverksky pr., 49
e-mails: adnaumov@corp.ifmo.ru, ilyapopov27@gmail.com

Abstract. The aim of this work is to study the applicability of the method of event bush in the field of information security. As a result, a model is built that identifies internal threats to a transaction. Developed model appears to be applicable in various situations in many fields where unusual values of any parameter should be identified and handled. Ultimately, the activity diagram-based approach to visualization of threats may lead to a cross-disciplinary classification of hazards and threats based on their formal properties.

Keywords: *event bush; model; methodology; information security; security threats.*

В обширной категории систем, созданных человеком – технических, социальных, экономических и, возможно, иных – можно выделить класс, характеризующийся следующим свойством. В системах данного класса происходит импульс, состоящий в передаче полезных вещества, энергии или информации от заданного отправителя заданному получателю, и действуют различные обстоятельства, способные внести изменения (как полезные, так и вредоносные) в процесс передачи этого импульса. Таким образом, поведение импульса описывается как переход системы из одного состояния в другое, не совместимое с предыдущим. К системам рассматриваемого класса относятся экономические, политические, юридические, информационные, психологические и физические системы. Роль импульса в них играют, соответственно, операция, состоящая в переводе денежных средств с одного счёта на другой, сделка купли-продажи; группа логически объединённых последовательных операций по работе с данными, обрабатываемая или отменяемая целиком; единица общения между двумя людьми и ключевое понятие транзакционной интерпретации квантовой механики.

Очевидно, эффективность функционирования этих систем всегда представляет практический интерес. В то же время, ввиду их разнообразия крайне затруднительно подобрать единую методологию, которая бы позволяла показать все варианты их поведения. Данная методология может быть только формальной. В то же время, для применения математической формализации нужно достаточно глубокое понимание того, с какими математическими объектами следует сопоставить импульсы и обстоятельства, на них влияющие, и как описать отношения между этими объектами, специфические для рассматриваемых систем.

Аппарат классической логики (логики предикатов) позволяет формализовать информацию без обращения к математической формализации, обращаясь к смыслам понятий, воспринимаемыми на естественном языке. Поиск общности смыслов представляется более простой задачей, нежели поиск математических свойств. Тем не менее, моделирование данных систем на языке логики предикатов наталкивается на трудность, которая едва ли преодолима в рамках этой логики: приведённое выше описание перехода, является прямым нарушением одного из её фундаментальных принципов – закона противоречия.

Единственным известным нам решением является методология инженерии динамического знания. Данная методология, несмотря на свою новизну и недостаточную проработанность, предлагает аппарат формализации смыслов подобно классической логике предикатов, но при этом позволяет моделировать смену взаимоисключающих состояний. При этом, формализуя частный случай, она может дать выводы, релевантные и для общего случая (систем с полезным импульсом).

СПИСОКЛИТЕРАТУРЫ

1. Diviacco P., Pshenichny C.A., Carniel R., Khrabrykh Z.V., Shterkhun V.L., Mouromtsev D.I., Guzman S.R., Pascolo P.B. Organization of a geophysical information space by using an event-bush-based collaborative tool//Earth Science Informatics, IET - 2015, Vol. 8, No. 3, pp. 677-695.
2. Mouromtsev D.I., Pshenichny C.A., Yakovlev A.V. Semantic and structural delineation of market scenarios by the event bush method//Decision Support Systems, IET - 2014, Vol. 57, No. 1, pp. 34-41.
3. Pshenichny C., Mouromtsev D. Grammar of Dynamic Knowledge for Collaborative Knowledge Engineering and Representation//Collaborative Knowledge in Scientific Research Networks, IET - 2015, No. Chapter 16, pp. 323-354.

УДК 004.056.53

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ПРИМЕРЕ ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ

Сазонов Антон Борисович, Немченко Алексей Алексеевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, ул. Большая Морская, 67, лит. А
e-mails: sazonov-anton@mail.ru, nemchenko_aleks@mail.ru

Аннотация. Работапосвящена системам контроля и управлениям доступа, развернутых в учебных заведениях высшего образования. Рассмотрены основные проблемы, которые помогает решить установка СКУД.

Ключевые слова: *системы контроля и управления доступом*.

ACCESS CONTROL AND MONITORING SYSTEM, FOR EXAMPLE, A HIGHER EDUCATION INSTITUTION

Sazonov Anton,Nemchenko Aleksey
St. Petersburg State University of Aerospace Instrumentation
Russia, St. Petersburg, str. Bolshaya Morskaya, 67, lit. A
e-mails: sazonov-anton@mail.ru, nemchenko_aleks@mail.ru

Abstract. The paper is devoted to access control systems and administrations deployed in educational institutions of higher education. The main problems that solve the installation of ACS.

Keywords: *access control system.*

Система контроля и управления доступом – это комплекс программно-аппаратных средств безопасности нацеленных на ограничение и регистрацию объектов(человек,машина) на вход и выход из заданной территории через точки прохода,такие, как КПП, двери и ворота. Основную роль,которую выполняет СКУД - управление доступом на заданную территорию. СКУД позволяет разграничивать доступ на заданную территорию и идентифицировать лицо,имеющую к ней доступ. СКУД состоит из считывателя,контроллера,конвертера среды и магнитного замка,а для идентификации объекта использует идентификатор – ключ,карта или брелок [1].

Рассматривая проекты системы контроля и управления доступом (далее – СКУД),можно сделать вывод,что на сегодняшний день возможностиСКУД остаются недооценёнными. СКУД позволяет устранить несколько проблем крупных организаций. Одна из таких проблем многопользовательский доступ к лекционным аудиториям учебных заведениях высшего образования. Для того, чтобы начать проводить лекцию преподавателю необходимо взять ключ от аудитории в бюро пропусков и вернуться в аудитории. В данном случае это может занимать дополнительное время, так как если у другого преподавателя была пара в этой же аудитории раньше,то сначала придется дождаться ключа,а уже после этого начинать проведение пары. СКУД решает данную проблему тем,что преподаватель сможет использовать свой личный пропуск как ключ к магнитному замку. В данном случае СКУД позволяет сформировать базу для контроллера в соответствие с расписанием преподавателя.

Следующую проблема, которую поможет решить СКУД – это возможность отслеживания посещения пар студентами. Для реализация такой возможности предлагается поставить либо промышленный считыватель с мощной антенной,либо считыватель большего радиуса действия. В данном случае преподаватель всегда будет иметь возможность просмотреть электронный журнал и проверить посещаемость конкретного студента. Так же СКУД может помочь реализовать возможность для временного доступа по индивидуальной ключ-карте к аудитории, в которой преподаватель не ведет пары, но ему нужно заменить его коллегу [2].

СКУД предоставляет широкие возможности по настройке и оптимизации рабочего процесса. На примере системы, разрабатываемой для вуза, можно убедится,что СКУД позволяет интегрировать себя в любую систему. Благодаря установке СКУД снижаются эксплуатационные расходы на поддержания в работе механических замков. Подобная система сэкономит значительное время и позволит преподавателям начинать пары вовремя. Это улучшит как качество рабочей среды, так и производительность труда,следовательно, повысит качество усвоения учебного материала студентами.

СПИСОК ЛИТЕРАТУРЫ

1. Национальный стандарт РФ ГОСТ Р 51241-2008 "Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 17 декабря 2008 г.) - 430 – с/
2. Примеры проектов СКУД [Электронный ресурс]. – URL:http://www.cleper.ru/project/category/kontrol-dostupa.php.– (Дата обращения: 20.09.2017)/

УДК 004

РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД К ПРОВЕДЕНИЮ И ОБЕСПЕЧЕНИЮ ВНУТРЕННЕГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Созинова Екатерина Николаевна
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mail: s.ekaterina-nik@mail.ru

Аннотация. Рассматривается влияние рисков на информационную безопасность организаций, важность и необходимость риск-ориентированного подхода к аудиту информационной безопасности.

Ключевые слова: *информационная безопасность; риск; аудит; управление информационной безопасностью.*

A RISK-BASED APPROACH TO CONDUCTING AND ENSURING OF INTERNAL AUDIT OF INFORMATION SECURITY

Sozinova Ekaterina
ITMO University
Russia, St. Petersburg, Kronverkskiy pr., 49
e-mail: s.ekaterina-nik@mail.ru

Abstract.Influence of risks on information security of the organizations, importance and need risk - the focused approach to audit of information security is considered**.**

Keywords: *information security; risk; audit; information security management.*

На данный момент наиболее часто можно услышать словосочетание «риск-ориентированный аудит». Риск-ориентированный аудит – это анализ и оценка аудиторского риска, это риск, что аудитор выразит ненадлежащее аудиторское мнение. Словосочетание «риск-ориентированный подход к проведению аудита информационной безопасности» - имеет совершенно другой смысл. Анализ литературы, посвященной проблемам риск-ориентированного подхода к проведению аудита, позволяет сделать вывод о том, что к настоящему времени, еще не сформировалось точное определение данного термина и структура подобного аудита. В настоящее время, данное словосочетание в таком виде используется очень редко.

Наиболее часто под риск-ориентированным подходом к проведению аудита понимается:

– аудит посредством применения всех методов риск-менеджмента;

– аудит, направленный на риски и процесс управления рисками в качестве целей аудита;

– это методология, позволяющая соединить аудит и общую систему управления рисками организации;

– это основанный на риске аудит, позволяющий менеджменту организации получить независимое и объективное мнение, на каком уровне происходит управление рисками.

В том, что риски играют очень важную роль, сомнений не возникает. Раньше это были кредитные, финансовые, экономические, коммерческие и производственные риски. Теперь, с развитием информационного общества, появился и новый вид риска – информационный риск. Управление собственными информационными рисками — важнейшая задача любой организации. Риск присутствует в любой экономической деятельности и без должного внимания к данной области, не может существовать ни один бизнес. Существует бесчисленное множество видов и типов риска, поэтому любая классификация рисков весьма условна, так как границу между отдельными видами риска можно провести весьма приблизительно. Многие риски взаимосвязаны, и изменения в одном из них, вызывают изменения в другом, но все они, в конечном счете, влияют на результаты деятельности организации и соответственно требуют оценки и управления.

Особенностью риска ИБ является то, что он зависит от большого количества факторов. Из всех рисков, риски ИБ наиболее сложные по своей природе, имеют самую большую неопределенность как по рисковым событиям, так и по наносимому ущербу. Поэтому факторные модели рисков ИБ имеют большую размерность и разнообразные причинно-следственные связи и отношения по сравнению с другими рисками.

Управление рисками является фундаментальным элементом в управлении организацией. Управление рисками внутри организации дает достаточно много преимуществ в результате своего структурированного, последовательного и скоординированного подхода. Именно поэтому, на наш взгляд, аудит информационной безопасности должен быть ориентирован на информационные риски. А в качестве объектов аудита должны рассматриваться не только финансовые документы, но и бизнес-процессы, и бизнес-среда, и связанные с ними риски.

В современных условиях выдвигаются дополнительные требования к процедурам и методам обеспечения и проведения аудита информационной безопасности. Инструментарием для проведения аудита должна стать теория управления рисками и выстроенная на ее базе методология внутреннего

контроля и аудита, что позволит своевременно выявлять и анализировать проблемы организации, формировать рациональный план проверки и эффективно распределять ресурсы. В связи с этим, необходимо использовать новейшие методики и научно-обоснованные методы выявления рисков, проведения оценки и ранжирования рисков по степени значимости, наличие критериев выбора эффективных методов управления информационными рисками.

Использование и совершенствование существующих методик и моделей выявления актуальных для организации рисков, их качественной и количественной оценке, управления внутренними рисками, позволит организациям снизить свои риски с одновременным повышением качества выполняемых работ, повысить эффективность систем обеспечения информационной безопасности, выполнить требования законодательства и внутренних регламентирующих документов, а также усилить предупредительный характер работы по выявлению источников рисков, уязвимостей и угроз.

Основываясь на вышеперечисленных факторах и анализах, можно уточнить и сформулировать понятие «риск-ориентированный подход к проведению аудита информационной безопасности».

Риск ориентированный подход к аудиту информационной безопасности – это когда обеспечение и проведение аудита информационной безопасности базируется и ориентируется на информационных рисках организации.

При таком подходе на основе расчетно-аналитических методов производится анализ и оценка информационных рисков, что позволяет получить объективные качественные и количественные оценки о текущем состоянии информационной безопасности организации. Опираясь на полученные в ходе аудита результаты, аудитор определяет для организации индивидуальный набор требований информационной безопасности, в наибольшей степени учитывающий особенности организации, среды ее функционирования и существующие в данной среде уязвимости и угрозы информационной безопасности.

Используя риск-ориентированный подход к проведению аудита информационной безопасности, можно:

– оценить текущее состояния информационной безопасности организации;
– выявить недостатки и определить направления развития системы защиты информации;
– систематизировать уязвимости, угрозы и риски информационной безопасности организации;
– спрогнозировать и минимизировать влияние рисков, угроз и уязвимостей, а также управлять их влиянием на бизнес-процессы организации;
– оценить степени соответствия ИБ организации выбранным критериям аудита;
– провести контроль эффективности вложений в обеспечение информационной безопасности организации;
– проконтролировать и оценить реализацию мероприятий по обеспечению информационной безопасности организации;
– и многое другое.

Таким образом, аудит информационной безопасности, основанный на риск-ориентированном подходе позволит руководителям организации получить взгляд со стороны на деятельность компании в целом, а также понять, какие шаги необходимо предпринять для повышения эффективности ее работы.

Аудит информационной безопасности, основанный на риск-ориентированном подходе позволяет дать оценку защищенности компании, выявить риски, создать и (или) скорректировать план мероприятий по минимизации рисков, улучшить взаимодействие отделов, ответственных за контроль и управление рисками и т.д.

Риск-ориентированный подход к аудиту информационной безопасности в данный момент времени и в ближайшие десятилетия – будет наиболее правильным и эффективным.

СПИСОК ЛИТЕРАТУРЫ

1. Зикратов И. А., Одегов С. В., Смирных А. В. Оценка рисков информационной безопасности в облачных сервисах на основе линейного программирования//Научно-технический вестник информационных технологий, механики и оптики. 2013 год, том 13, номер 1, стр. 141-144.
2. Шаго Ф. Н., Зикратов И. А. Методика оптимизации планирования аудита системы менеджмента информационной безопасности// Научно-технический вестник информационных технологий, механики и оптики. 2014 год, том 14, номер 2, стр. 111-117.
3. Арустамов С. А., Генин М. Г. Методы снижения рисков потерь доступности программного обеспечения критических информационных систем// Научно-технический вестник информационных технологий, механики и оптики. 2012 год, том 12, номер 4, стр. 131-136.

УДК 004

МЕТОД ПРОВЕДЕНИЯ ВНУТРЕННЕГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Созинова Екатерина Николаевна
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mail: s.ekaterina-nik@mail.ru

Аннотация. Автор коротко описывает разработанный им метод проведения аудита информационной безопасности, используемый при риск-ориентированном подходе к проведению аудита информационной безопасности. В докладе описывается выбранный алгоритм проведения аудита, основные этапы и параметры оценки, приводится итоговая формула для расчета уровня обеспечения информационной безопасности.

Ключевые слова: *информационная безопасность; риск; аудит; управление информационной безопасностью.*

METHOD OF CONDUCTING INTERNAL AUDIT OF INFORMATION SECURITY OF ORGANIZATION

Sozinova Ekaterina
ITMO University
Russia, St. Petersburg, Kronverkskiy pr., 49
e-mail: s.ekaterina-nik@mail.ru

Abstract. The author briefly describes the developed method for conducting the audit of information security used in a risk-focused approach to auditing of information security. The report describes the selected algorithm of audit, main stages and parameters of evaluation, is the final formula for the calculation of the level of information security.

Keywords: *information security; risk; audit; information security management.*

Обеспечение информационной безопасности (ИБ) - является одной из самых важных задач любой организации. Сейчас, в период нарастающей информатизации, глобализации и жёсткой конкуренции, этот вопрос становится особенно «острым» и актуальным. Для того, чтобы гарантировать эффективное обеспечение информационной безопасности организаций, нужен серьёзный, систематизированный и комплексный подход. Немаловажную роль в этом подходе играет аудит информационной безопасности.

Несмотря на то, что проведение аудита информационной безопасности - это новое и до конца не исследованное направление, в настоящее время данная услуга становится все более востребованной на рынке услуг информационной сферы.

Цель работы: разработка метода внутреннего аудита информационной безопасности для оценки текущего состояния информационной безопасности организаций.

Основными факторами актуальности данной исследовательской работы являются:

1. В стране отсутствует единая система взглядов на государственное регулирование процессов аудита информационной безопасности организаций;
2. В сфере информационной безопасности не сформировалась единая и общепризнанная терминология;
3. Нет универсальных, общепринятых и утвержденных методов проведения аудита информационной безопасности организаций;
4. Существующие разработки по проведению аудита информационной безопасности являются узконаправленными и «закрытыми» для общего пользования;
5. Как показывает практика, и заказчики, и поставщики, очень часто, понимают суть этой услуги по-разному.

Алгоритм проведения внутреннего аудита информационной безопасности состоит из четырех основных этапов: подготовительный, исследовательский, оценочный и заключительный. Эти этапы, в свою очередь, подразделяются на подэтапы: инициирование проведения аудита, планирование аудита, общее исследование организации, оценка угроз, анализ и оценка рисков, определение уровня обеспечения ИБ организации, разработка рекомендаций, составление аудиторского отчета.

К сожалению, в настоящее время, лишь, незначительное количество организаций проводят внутренний аудит информационной безопасности. Некоторые не понимают необходимость этого процесса, а те, кто понимают и видят пользу, эффективность и необходимость проведения аудита, сталкиваются с одной очень значительной трудностью: нет общепринятого метода обеспечения и проведения внутреннего аудита информационной безопасности организации. Такого метода, чтобы он был признан и закреплен на законодательном уровне; чтобы этим методом могли пользоваться внутренние сотрудники без специального длительного и дорогостоящего обучения; чтобы он учитывал интересы бизнеса и мог быть не только общим, но и локальным.

Управление информационными рисками, построение комплексной системы управления информационной безопасностью и регулярное проведение внутреннего аудита ИБ – это для каждой организации шаг на качественно иной уровень корпоративного управления, а в некоторых случаях, – решающее конкурентное преимущество. Несомненно, положительный эффект от проведения внутреннего аудита по разработанному методу будет очевидным. И это гораздо дешевле, чем привлекать сторонних специалистов или восстанавливать систему после нарушения информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Зикратов И. А., Одегов С. В., Смирных А. В. Оценка рисков информационной безопасности в облачных сервисах на основе линейного программирования//Научно-технический вестник информационных технологий, механики и оптики. 2013 год, том 13, номер 1, стр. 141-144.
2. Шаго Ф. Н., Зикратов И. А. Методика оптимизации планирования аудита системы менеджмента информационной безопасности// Научно-технический вестник информационных технологий, механики и оптики. 2014 год, том 14, номер 2, стр. 111-117.
3. Арустамов С. А., Генин М. Г. Методы снижения рисков потерь доступности программного обеспечения критических информационных систем// Научно-технический вестник информационных технологий, механики и оптики. 2012 год, том 12, номер 4, стр. 131-136.

УДК 004

ПРОБЛЕМА НЕСООТВЕТСТВИЯ СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ СОВРЕМЕННЫМ ТРЕБОВАНИЯМ МЕР ФИЗИЧЕСКОЙ ЗАЩИТЫ

Федорова Алёна Владимировна[1], Алексеев Дмитрий Станиславович[2]
[1] Университет ИТМО
Россия, Санкт-Петербург, Кронверскийпр., 49
[2]Военная академия радиационной, химической и биологической защиты им. Маршала Советского Союза С. К. Тимошенко
Россия, Кострома, ул. Горького, 16
e-mails: fedorovaits@gmail.com, alex-dmst@yandex.ru

Аннотация. В работе рассмотрена проблема приведения в соответствие современным требованиям мер физической защиты службы информационной безопасности организаций, особенности этого процесса в учреждениях здравоохранения.

Ключевые слова: *информационная безопасность; персональные данные; защита информации; медицинская организация.*

THE PROBLEM OF NON-COMPLIANCE OF MEDICAL ORGANIZATIONS' INFROMATION SECURITY SERVICES WITH MODERN REQUIREMENTS OF PHYSICAL PROTECTION MEASURES

Fedorova Alyona[1], Alekseev Dmitriy[2]
[1] St. PetersburgNational Research University of Information Technology, Mechanics and Optics
Russia, St. Petersburg,Kronverksky pr.,49
[2]Kostroma Nuclear, Biological and Chemical Protection Military Academy named after Marshal S. Timoshenko,
Russia, Kostroma, Gorkogo str., 16
e-mails: fedorovaits@gmail.com, alex-dmst@yandex.ru

Abstract. This article describes the problem of modernizing physical protection measures in organizations' information security services and special cases of this process in medical organizations.

Keywords: *information security; personal data; information protection; medical organization.*

Электронный документооборот всё надежнее входит в жизнь учреждений здравоохранения. Но создание в медицинской организации информационной системыпорождает дополнительные уязвимости и угрозы. Большинство учреждений имеет устаревшую службу защиты или же полное ее отсутствие, этим обусловлена актуальность данной работы.

Процесс приведения в соответствие современным требованиям службы информационной безопасности состоит из трёх этапов.

На первом этапе исследования определены современные требования мер физической защиты для учреждений здравоохранения в целом.

Второй этап представляет собой сбор и анализ информации об уже существующих мерах защиты в конкретной организации, выбранной для изучения. На этом этапе построены модель системы информационной безопасности, модели угроз и нарушителя.

На третьем этапе была проведена оценка уровня защищенности медицинской организации путем сравнения функционирующих мер защиты с требованиями современного законодательства в сфере информационной безопасности, а также перечень рекомендаций для организации.

Результатом работы является заключение об уровне мер, организованных службой информационной безопасности медицинской организации. Оно служит основой для разработки плана мероприятий по защите от угроз в соответствии с современными требованиями.

СПИСОК ЛИТЕРАТУРЫ

1. Зикратов И. А., Одегов С. В., Смирных А. В. Оценка рисков информационной безопасности в облачных сервисах на основе линейного программирования//Научно-технический вестник информационных технологий, механики и оптики. 2013 год, том 13, номер 1, стр. 141-144.

УДК 004.056

МЕТОДИКА ПРЕДВАРИТЕЛЬНОЙ ОБРАБОТКИ ГРАФИЧЕСКИХ ОБЪЕКТОВ ДЛЯ ЗАДАЧИ ИДЕНТИФИКАЦИИ В ВИДЕОПОТОКЕ

Шевченко Денис Алексеевич
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mail: dashevchenko@corp.ifmo.ru

Аннотация. В статье рассматривается задача подготовки исходных данных для последующей идентификации объектов в видеопотоке, проведено исследование взаимодействия различных методов цифровой обработки изображений между собой. Разработан метод улучшения визуального качества видео с низким динамическим диапазоном. В результате работы сформирован определенный порядок операций, применяемых к видеоизображению, позволяющий добиться наилучшего результата.

Ключевые слова: *обработка изображений; идентификация объектов.*

METHOD OF PRELIMINARY PROCESSING OF GRAPHIC OBJECTS IN THE VIDEO SEQUENCE FOR IDENTIFICATION

Shevchenko Denis
St. Petersburg State University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverkskiy pr.,49
e-mail: dashevchenko@corp.ifmo.ru

Abstract. The article deals with the problem of preparing the initial data for the subsequent identification in a video stream, conducting studies of the interaction of various methods of digital image processing.The method to improving the visual quality of video with a low dynamic range was developed. As a result of the work, the order of operationsis formed which allows to achieve the best result.

Keywords: *imageprocessing; object identification.*

Введение. Постоянно набирающий темпы технический прогресс приводит к повсеместному распространению устройств видеофиксации. Наряду с портативными цифровыми камерами увеличивается количество систем видеонаблюдения, цифровых видеорегистраторов, телефонов с камерами. Все это способствует повышению качества цифровых изображений и видеоматериалов. Несмотря на то, что качество технологии цифровых камер постоянно улучшается, цифровые изображения, используемые в криминалистических исследованиях, часто не являются релевантными. Такие проблемы, как плохое разрешение, низкая контрастность, неточное воспроизведение цвета, размытие и шум, являются типичными при использовании цифровых изображений. Методы улучшения качества изображения могут быть использованы для решения многих из этих проблем.

Производители программного обеспечения для информационных систем предоставляют решения подобного рода, однако предлагаемые ими алгоритмы разрознены и требуют детальной настройки. Исследователи не ставят своей целью создать всеобъемлющую и универсальную технологию обработки фото- и видеоизображений с целью улучшения их визуального качества, а решают узкие конкретные задачи. Произвольное объединение множества разнородных алгоритмов в рамках единой технологии приводит к падению качества обработки изображений из-за слабой согласованности отдельных алгоритмов.

Улучшение изображения является общепринятой практикой в области компьютерной криминалистики и широко используется в экспертно-криминалистических приложениях, таких как реконструкция места преступления, фотограмметрия и биометрический анализ, включая идентификацию субъекта по лицу и отпечатку пальца. Когда к изображению применяется множество операций, каждая операция будет оказывать влияние на любую будущую обработку изображения. Применение одних и тех же методов улучшения изображения к одному и тому же изображению при одинаковых настройках в неправильном порядке может привести к полной потере достоверности изображения или созданию характеристик, которых нет в исходных графических данных, включая такие артефакты, как зашумление или ложные края.

Визуальные компоненты цифровых изображений представляют собой матрицу числовых значений. Операции обработки изображений используют алгоритмы математического управления численными значениями. Поскольку эти алгоритмы работают строго определенным образом, можно предсказать их поведение. Изучая основные процессы алгоритмов обработки изображений, можно предсказать, как они реагируют на различные свойства изображения и тем самым установить такой порядок их применения, при котором достигается наилучший результат. Отсюда возникает вопрос, какой результат в данном случае будет наилучшим. Разумеется, такие ответственные области, как экспертно-криминалистические исследования, требуют, чтобы по возможности использовались релевантные методы. Однако определение релевантного метода может быть сложным, поскольку релевантность субъективна и становится значимой только в отношении конечной цели. Например, подходы, которые могут быть релевантными в обработке изображений для создания специальных эффектов фильма, могут быть неприменимы для криминалистических целей.

Таким образом, мы будем определять улучшение исследуемого изображения как улучшение визуального внешнего вида изображения таким образом, чтобы оно стало более полезным в дальнейших научных исследованиях. В соответствии с этим определением любой порядок операций для обработки изображения без искажения отображаемого контента будет считаться более релевантным, чем какой-либо другой. Традиционно порядок, в котором применяются алгоритмы улучшения изображений, не является согласованным и, более того, считается невозможным или нецелесообразным создание определенного порядка операций для улучшения цифрового изображения. Целью исследования является создание такого порядка и обоснование его применимости ко многим распространенным вариантам использования методов улучшения изображений.

В ходе исследования произведены формирование обобщенного подхода к улучшению качества видеоизображения, разработка метода обработки видеоданных, разрешающего проблему несогласованности существующих методов повышения визуального качества видеоизображений, на основе методов дискретной обработки сигналов, цифровой обработки изображений. Практическая значимость исследования состоит в применимости разработанной методики при проведении расследований инцидентов, требующих исследования видеоматериалов.

Большинство методов улучшения визуального качества изображений, могут применяться последовательно для достижения наилучшего эффекта. Однако процессы шумоподавления и тональной компрессии тесно связаны между собой и в некоторых случаях не могут выполняться последовательно. Одним из самых сложных случаев при улучшении визуального качества видеоизображения является низкий динамический диапазон яркостей изображения. В этом случае значения интенсивности шумов могут быть сопоставимы со значениями интенсивности сцены изображения. Такая ситуация возникает, например, при видеосъемке в обстановке с низкой освещенностью.

Прямое растяжение динамического диапазона видео с низким освещением провоцирует появление различных нежелательных эффектов, таких как усиление шума, насыщенность интенсивности и снижение разрешения. Таким образом, перед тем, как сжать динамический диапазон, необходимо выполнить подходящую процедуру шумоподавления. Однако, несмотря на то, что перед шагом тональной компрессии удалится значительное количество шума, шум, усиленный на этапе тональной компрессии, должен быть удален с помощью подходящего метода шумоподавления. Предлагаемый метод улучшения видеоизображения основан на алгоритмах улучшения изображений. Процесс показан на рис. 1.

Проблема с видео с низким освещением заключается в том, что содержимое сложно различить. В нормальных условиях может использоваться пространственно-временная фильтрация, однако в условиях низкой освещенности из-за низкого динамического диапазона пространственно-временная фильтрация приводит к размытию и искажению фона вокруг движущихся объектов. Методы регулировки динамического диапазона, непосредственно примененные к видео, приведут к усилению шума наряду с улучшением видимости. Предлагаемый метод улучшения изображения используется для повышения видимости объектов в видео с низким тональным диапазоном и предотвращения этих нежелательных эффектов.

Метод состоит из трех этапов, которые применяются последовательно. Изначально применяется временная фильтрация перед регулировкой динамического диапазона для устранения шума в неподвижных областях. Затем динамический диапазон изображения растягивается путем тональной компрессии с целью повышения видимости.

Наконец, выполняется пространственное шумоподавление для устранения усиленного на этапе тональной компрессии шума.

Поскольку видеофрагменты коррелированы во времени, шум может быть эффективно уменьшен за счет временной фильтрации. Для удаления временного шума без размытия движения реализована модель фильтра с компенсацией движения с применением фильтра Калмана.

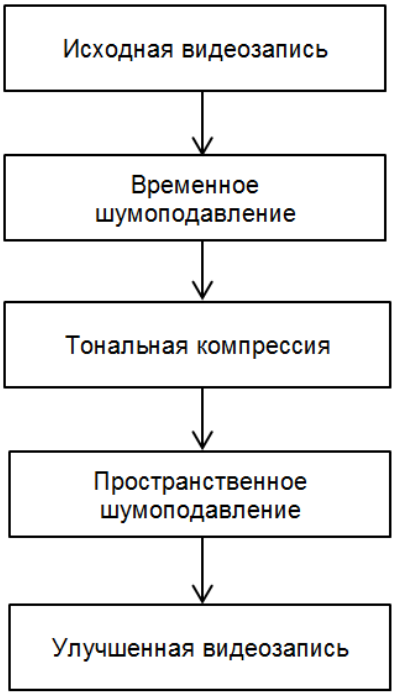


Рис.1. Метод улучшения визуального качества видеозаписи

Для выбора наиболее подходящего метода тональной компрессии были сформированы три модели метода и исследована их эффективность. Существует три различных подхода к осуществлению тональной компрессии:

– глобальное выравнивание гистограммы – алгоритмы данной группы методов тональной компрессии регулируют контрастность глобально по всему изображению, не учитывая локальные особенности изображения;

– локальное выравнивание гистограммы – алгоритмы данной группы методов используют нелинейные кривые преобразования гистограмм, учитывая локальное распределение полутонов;

– адаптивная эквализация гистограмм с ограничением контраста;

Из первой группы методов был выбран алгоритм гамма-коррекции – Модель 1.

Из второй группы методов был выбран алгоритм улучшения темных изображений, учитывающий их содержимое – Модель 2.

Из третьей группы был выбран метод адаптивной эквализации с ограничением контраста (CLAHE) – Модель 3.

Видео с низким динамическим диапазоном сначала подвергается временной фильтрации, затем тональной компрессии, и в завершение фильтруется в пространственной области. Несмотря на то, что значительное количество шума ослабляется после временного шумоподавления, оставшийся шум усиливается на этапе тональной компрессии. Для пространственного шумоподавления в работе используется алгоритм нелокальных средних, который измеряет сходство между соседним и опорным блоком.

Алгоритм нелокальных средних вычисляет средневзвешенное значение пикселей в пространстве, рассматривая сходство между пикселями для понижения шумов изображения. Несмотря на то, что алгоритм нелокальных средних дает хорошие результаты, для его работы требуется большое количество вычислений, так как в процессе работы вычисляются веса для всей окрестности. В работе используется модифицированный фильтр нелокальных средних для упрощения процесса пространственного шумоподавления и сокращения вычислений.

Сравнение результатов работы трех моделей представлены в табл. 1.

Таблица 1

Результаты сравнения моделей

Измерение	Входные данные	Модель 1	Модель 2	Модель 3
PSNR	6,9	18,51	18,72	18,55
SSIM	0,12	0,61	0,64	0,55

Таким образом, в предлагаемом порядке операций по улучшения видеоизображений в качестве 5-го шага в табл. 2 будет использоваться второй вариант метода.

Основной целью установления порядка операций является обеспечение качества обработки видеоданных. Порядок операций устанавливает правила, которые уменьшают вероятность появления ошибки вследствие человеческого фактора и способствуют проведению надежного анализа. Если прядок является обоснованным, может быть повышена уверенность в том, что эксперты будут создавать визуально сопоставимые результаты и что эти результаты с меньшей вероятностью искажают исходные данные. В табл. 2 представлен предлагаемый порядок действий.

Таблица 2

Порядок действий для улучшения видеоизображения

Этап	Наименование операции
1	Визуальный анализ
2	Корректировка артефактов видео
3	Изменение размера
4	Усреднение кадров / Усиление разрешения
5	Корректировка контрастности / Шумоподавление
6	Корректировка размытия
7	Корректировка искажения
8	Корректировка резкости

В результате исследований, проведенных в данной работе, было обнаружено, что порядок применения определенных методов улучшения изображений может повлиять на визуальную точность обрабатываемого изображения. Проводя тестирование различных комбинаций методов обработки изображений, было определено следующее: чересстрочное видео не может быть точно приведено в соответствие с прогрессивной разверткой после применения таких операций, как интерполяция, корректировка размытия и корректировка искажения.

Шум может негативно повлиять на алгоритмы устранения размытости, регулировки контрастности и увеличения резкости. Размытость негативно влияет на видимость после увеличения резкости и корректировки цвета. Корректировка размытости не может быть корректно выполнена после корректировки искажения. Наконец, устранение размытости и корректировка цвета могут помочь определить области, которые могут быть улучшены путем увеличения резкости.

В результате исследования был разработан такой порядок операций для обработки графических данных, при котором увеличивается эффективность каждого метода улучшения изображений.

Вывод. Предлагаемый порядок операций по улучшению изображений направлен на нахождение оптимального баланса между повышением информативности изображения и уменьшением артефактов посредством исследования свойств изображений и взаимодействия методов обработки изображений между собой.

СПИСОК ЛИТЕРАТУРЫ

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений: Учебное пособие – М.: Техносфера, 2012, 1104с.
2. Оппенгейм А., Шафер Р. Цифровая обработка сигналов: Учебное пособие – М.: Техносфера, 2012, 1048с.

УДК 004.052.42

ОБНАРУЖЕНИЕ МЕСТ НАРУШЕНИЯ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ РЕСУРСОВ В ПРОГРАММНОМ КОДЕ

Цветков Лаврентий Викторович, Спивак Антон Игоревич
Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр.,49
e-mails: lavrentii.tsvetkov@corp.ifmo.ru, anton.spivak@gmail.com

Аннотация. В статье рассмотрен способ обнаружения дефектов программного обеспечения, связанных с небезопасным использованием различных программных ресурсов. На основе предложенной модели построен метод поиска, способный учитывать возможность различного состояния ресурса относительно операций управления, примененных внутри условных выражений. Представлены предлагаемые правила и ох описания.

Ключевые слова: *дефекты ПО; системы типов; анализ программ.*

LOCATING VIOLATION OF SAFE SOFTWARE RESOURCE USE IN A PROGRAM

Tcvetkov Lavrentii, Spivak Anton
ITMO University
Russia, St. Petersburg, Kronversky pr., 49
e-mails: lavrentii.tsvetkov@corp.ifmo.ru, anton.spivak@gmail.com

Abstract. The article presents a method of detecting software defects, related to unsafe use of software resource. Based on proposed model, detection method was constructed that accounts for possible different resource state in respect to resource management operations applied in conditional statements. Inference rules for proposed method are shown and described.

Keywords: *software defects; type systems; program analysis.*

Введение.

При разработке программных продуктов немаловажным аспектом является обеспечение корректности работы создаваемых программ. Одной из причин возникновения различных ошибок, влияющих в том числе на защищенность программ, является нарушение заданного протокола взаимодействия с различного вида ресурсами. Несмотря на широкое распространение высокоуровневых языков, облегчающих разработку программ за счет автоматического управления памятью, в большинстве из них нет средств, обеспечивающих гарантированное освобождение других ресурсов.

Отсутствие таких механизмов обуславливает возможность проведения различного рода атак, например, атак вида «отказ в обслуживании». В данном случае ресурсом, на который может проводится атака, является дескрипторы сетевых соединений. Память, отведенная в операционной системе для хранения технических данных о соединениях ограничена, поэтому при некорректном или несвоевременном освобождении данного ресурса дальнейшее создание соединений может оказаться невозможным.Как было показано авторами ранее [1, 2], использование систем типов применительно к разработанной модели кода позволяет обнаруживать различные логические ошибки управления ресурсами. В рамках предложенного метода элементам построенной модели программного кода ставится в соответствие параметризованный маркер, называемый типом ресурса. Конкретные значения параметров маркера определяют возможность или невозможность использования соответствующих синтаксических структур в исходном коде программ.

Использование расширенной системы типов в дополнение к собственной системе типов исследуемого языка расширяет возможности метода и устраняет привязку к конкретному языку программирования. Необходимо отметить, что в качестве ресурсов могут выступать не только сущности, администрируемый операционной системой. При более общем толковании ресурсом могут названы, к примеру, контейнер с конфиденциальными данными пользователя или sql-запросы. В таком случае, в рамках предлагаемой модели возможно введение правил, вводящих дополнительные ограничения, соответствующие корректному использованию данного ресурса. Для примера с контейнером конфиденциальных данных таким ограничением может являться разрешение на запись этих данных только в каналы, имеющие признак доверенных, а для случая sql-запросов – требование предварительного экранирования данных, полученных от пользователя.

Описание метода.

В качестве модели программного кода выступает SSA-представление (Static Single Assignment form) программы, расширенное возможностью задания для элементов дополнительных типов-маркеров. Используя тот факт, что в данном представлении каждая переменная может быть присвоена лишь один раз, возможно значительно сократить количество правил вывода новых маркеров.

Для отслеживания состояния ресурса и связанного дескриптора мы будем использовать назначение меток переменным путем задания им соответствующих типов, имеющих, помимо типа самого значения, дополнительные индексы, позволяющие ограничивать область действия переменной без изменения её значения. Такие индексы называются фантомными[5].

Несмотря на неизменяемость значений самих переменных в SSA, возможно изменение типа самой переменной путем замены параметров типа. Это позволяет легко ограничить дальнейшую работу с переменной, а также соответствует семантике императивных языков, поскольку предыдущий определенный тип становится недоступным для использования. Особенно важно учесть в модели возможность создании копии дескриптора ресурса, поскольку необходимо обеспечить согласованность состояния между несколькими копиями или псевдонимами.

Для отслеживания состояния копий дескриптора будет использоваться тип $\Re$, имеющий два параметра. Первый параметр соответствует той переменной, из которой данный дескриптор был получен копированием, либо состоит из специального маркера N, соответствующему оригинальному дескриптору. Второй параметр необходим для обеспечения согласованности операций освобождения

ресурса и отслеживает количество копий-псевдонимов дескриптора. Определение типа дескриптора происходит согласно следующим правилам:

$$\frac{v \leftarrow \mathrm{open}(f)}{\Gamma \vdash v{:}\,\Re\mathrm{N1}}\,(OPEN) \tag{1}$$

$$\frac{\Gamma \vdash v{:}\,\Re v_0 i \quad v' \leftarrow v}{\Gamma \vdash v{:}\,\Re v_0(i+1), v'{:}\,\Re v1}\,(HCOPY) \tag{2}$$

$$\frac{\Gamma \vdash v{:}\,\Re v_0 i \quad v' \leftarrow \mathrm{dup}v}{\Gamma \vdash v'{:}\,\Re\mathrm{N1}}\,(COPY) \tag{3}$$

$$\frac{\Gamma \vdash v{:}\,\Re v_0(i+1) \quad \Gamma \vdash v'{:}\,\Re v1}{\Gamma \vdash v{:}\,\Re v_0 i}\,(SCOPE) \tag{4}$$

$$\frac{\Gamma \vdash v{:}\,\Re\mathrm{N1} \quad \mathrm{close}(v)}{\Gamma \vdash v{:}\mathrm{Null}}\,(CLOSE) \tag{5}$$

$$\frac{\begin{array}{rr}\Gamma \vdash b : \mathbf{bool} & \\ \Gamma, b \vdash e_1 : \tau_1 & \textbf{if } b \textbf{ then } \; s_1; v_1 \leftarrow e_1; s_1' \\ \Gamma, \mathbf{not}\, b \vdash e_2 : \tau_2 & \textbf{else } \; s_2; v_2 \leftarrow e_2; s_2'\end{array}}{\Gamma \vdash \varphi(b, v_1, v_2) : \Phi(b, \tau_1, \tau_2)}\,(\mathrm{IF}) \tag{6}$$

$$\frac{\Gamma \vdash v : \Phi(\mathbf{T}, \tau_1, \tau_2)}{\Gamma \vdash v : \tau_1}\,(\Phi\pi_1) \qquad \frac{\Gamma \vdash v : \Phi(\mathbf{F}, \tau_1, \tau_2)}{\Gamma \vdash v : \tau_2}\,(\Phi\pi_2) \qquad \frac{\Gamma \vdash v : \Phi(b, \tau, \tau)}{\Gamma \vdash v : \tau}\,(\mathrm{CONVERGE}) \tag{7}$$

$$\frac{\Gamma \vdash v : \mathbf{R\,N}\,1 \qquad \Gamma \vdash f : \mathbf{R\,N}\,1 \to \mathbf{Null}}{\Gamma \vdash f(v) : \mathbf{Null}, v : \mathbf{Null}}\,(\mathrm{TRANSFER}) \tag{8}$$

В дополнение к правилам (1-5) управления ресурсами, детально описанных в работе [2], представлены дополнительные правила, обеспечивающие работу метода в случае наличия разветвленной сети условных выражений.

Правило (6) соответствует определению типа ресурса при использовании операций управления внутри условных выражений. Типом условного выражения, представленного в SSA-форме в виде специальной функции φ является зависимый тип Φ, который сохраняет типы возможных исходов условного выражения в невычисленной форме. При помощи этого достигается возможность обнаружить места нарушения безопасного использования ресурсов, в которых нарушение происходит по причине неполного учета возможных путей исполнения программы.

Группа правил (7) отражает стандартные проекции зависимого типа Φ при условии известности в данной области программы истинности выражения, ставшего ранее причиной разделения состояния ресурса. Третье правило группы позволяет проигнорировать конкретное значение истинности условного выражения в случае эквивалентности результата относительно состояния ресурса.

Достаточно частой практикой является нарушение принципа одинаковой вложенности операторов управления ресурсом. В результате возникает необходимость обеспечить в рамках метода возможность передать ресурс в более глубокий уровень вложенности без увеличения счетчика псевдонимов в типе ресурса даже в тех случаях, когда создание таких псевдонимов следует из семантики языка. Такая передача ресурса является безопасной только в том случае, когда отсутствуют другие псевдонимы данного ресурса, что обеспечивается правилом (7). Дополнительно оно удостоверяет, что в оригинальной области видимости дальнейшая работа с данным дескриптором будет невозможна.

Заключение. Описанный метод позволяет провести поиск мест небезопасного использования ресурсов в условиях наличия операция управления различными ресурсами в разных ветвях условных выражений. Показана возможность расширенного толкования понятия ресурса, при котором данных подход может быть использован для широкого спектра объектов с похожими моделями взаимодействия. В результате исправления обнаруженных мест небезопасно использования ресурсов повышается качество программного обеспечения и его защищенность к различным угрозам.

СПИСОК ЛИТЕРАТУРЫ

1. Tsvetkov L., Spivak A. Utilizing type systems for static vulnerability analysis //Open Innovations Association and Seminar on Information Security and Protection of Information Technology (FRUCT-ISPIT), 2016 18th Conference of. – FRUCT, 2016. – С. 345-350.
2. Цветков, Л.В. Использование модели программного кода для обнаружения программных дефектов / Л.В. Цветков // Региональная информатика (РИ-2016): Труды конференции (Санкт-Петербург, 26-28октября 2016г.). - 2016. - С. 99-101

УДК 004.056

МОДЕЛЬ ОБНАРУЖЕНИЯ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ НА МУЛЬТИАГЕНТНЫЕ РОБОТОТЕХНИЧЕСКИЕ СИСТЕМЫ

Юрьева Радда Алексеевна, Тимко Андрей Сергеевич, Комаров Игорь Иванович

Университет ИТМО
Россия, Санкт-Петербург, Кронверкский пр., 49
e-mails: raddaiureva@corp.ifmo.ru, timko.andrew@gmail.com, komarov@cit.ifmo.ru

Аннотация. Целью исследования является разработка метода обнаружение скрытого деструктивного информационного воздействия (СДИВ) на мультиагентные робототехнические системы (МРТС). Принцип работы предлагаемого метода состоит в обнаружении несоответствия между текущим режимом работы МРТС и режимом работы, который отвечает штатной модели поведения данного алгоритма, так называемого «портрета». Несоответствие «портрету» рассматривается как информационная атака. Актуальность исследования определяется необходимостью обеспечения безопасного функционирования МРТС.

Ключевые слова: *информационная безопасность; роевые системы; мультиагентные системы; робототехнические системы; деструктивное воздействие; информационная атака.*

MODEL OF DETECTION OF DESTRUCTIVE IMPACT ON MULTI-AGENT ROBOTIC SYSTEMS

Iureva Radda, Timko Andrey, KomarovIgor
St. Petersburg State University of Information Technologies, Mechanics and Optics
Russia, St. Petersburg, Kronverksky pr., 49
e-mails: raddaiureva@corp.ifmo.ru, timko.andrew@gmail.com, komarov@cit.ifmo.ru

Abstract. The purpose of the study is to develop a method for detecting a hidden destructive information impact (SAD) on multi-agent robotic systems (MRTS). The principle of the proposed method is to detect a discrepancy between the current mode of operation of the MRTS and the mode of operation that corresponds to the regular model of the behavior of this algorithm, the so-called "portrait". The discrepancy "portrait" is considered as an information attack. The urgency of the study is determined by the need to ensure the safe operation of the MRTS.

Keywords: *information security; swarm systems; multi-agent systems; robotic systems; destructive impact; information attack.*

Поведение роя зависит от действий каждого его агента, более того поведение роботов является автономным и зависит от изучаемой окружающей среды, что делает выявление аномального поведения нетривиальной задачей безопасности. Существует риск незаметного случайного или преднамеренного проникновения роботов-нарушителей в рой с целью нарушения корректного поведения членов роя.

Основная часть. Метод идентификации деструктивного воздействия на МРТС, предлагаемый в данном исследовании, основывается на том, что известны некоторые признаки, характеризующие правильное или допустимое поведение объекта наблюдения. Под нормальным поведением понимается функционирование системы, при котором действия, выполняемые объектом, не противоречат политике безопасности.

Приоритетной целью нарушителя является скрытное деструктивное воздействие на мультиагентную робототехническую систему (МРТС). Случаи физического уничтожения и электромагнитного подавления с уровнем, которые вызывают нарушение нормального функционирования системы, в исследовании не рассматриваются. Условием, которое обязательно дабы обеспечить информационную безопасность служит сохранение единства функционирования оборудований МРТС и его устройств с остальными внешними составляющими.

Такие угрозы характеризуются нарушением режимов функционирования, или их вывод из работы. Как результат, может быть осуществлены: повышение вероятностей НСД, отказ в сервисе, искажение и потеря используемых ранее данных.

Отличие в «портрете» определим как множество точек, удовлетворяющих условию:

$$R(f,g) = \left[x \in X \middle| f(x) - g(x)\right] > T, \qquad (1)$$

где $f(x)$ – функция изменения значения информативного признака на каждом шаге итерации при отсутствии СДИВ, $g(x)$ – функция изменения значения информативного признака на каждом шаге итерации при наличии СДИВ, x – шаг итерации, T – некоторое пороговое значение.

Признаковое пространство для идентификации отклонения от безопасной модели поведения формируется из числа доступных измерению характеристик объекта или группировки объектов, которые отражают наиболее существенные свойства в ходе выполнения репрезентативных

алгоритмов. К признакам предъявляются требования: объективность, доступность (возможность получения), достаточность.

Определение совокупности и/или преобразования (минимально) достаточных признаков обеспечивает возможность для синтеза формальных алгоритмов обнаружения деструктивного воздействия, которые, в свою очередь, могут применяться для решения первой и второй частной задачи.

Научная новизна предлагаемого метода заключается в возможности обнаружения атак нового типа без модификации или обновления параметров модели, так как вторжение нарушителя в систему может быть описано как некоторое отклонение от штатного поведения.

СПИСОК ЛИТЕРАТУРЫ

1. Юрьева Р.А., Комаров И.И., Дородников Н.А. Построение модели нарушителя информационной безопасности для мультиагентной робототехнической системы с децентрализованным управлением // Программные системы и вычислительные методы - 2016. - № 1(14). - С. 42-48
2. Каляев, И.А. Модели и алгоритмы коллективного управления в группах роботов / И. А. Каляев, А. Р. Гайдук, С. Г. Капустян. - М. : Физматлит, 2009. - 278 с.
3. Y. U. Cao, A. S. Fukunaga, and A. B. Kahng, “Cooperative mobile robotics: antecedents and directions,” Autonomous Robots, vol. 4, no. 1, pp. 226–234, 1997., C. Ronald Arkin, Behavior-Based Robotics, MIT Press, Cambridge, Mass, USA, 1998
4. K. Fujibayashi, S. Murata, K. Sugawara, and M. Yamamura, “Self-organizing formation algorithm for active elements,” in Proceedings of the 21st IEEE Symposium on Reliable Distributed Systems (SRDS '02), pp. 416–421, IEEE Computer Society, Washington, DC, USA, October 2002.
5. Юрьева Р.А., Мальцева Н.К., Кульпина А.Д., Юшков К.С., Иванова А.С. Особенности конструирования электромеханического привода // Наука и бизнес: пути развития - 2015. - № 10(52). - С. 21-23
6. Юрьева Р.А., Комаров И.И., Дранник А.Л., Масленников О.С. Постановка задачи обеспечения информационной безопасности роевых робототехнических систем // Наука и бизнес: пути развития - 2015. - № 3(45). - С. 66-72

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОБЛЕМЫ УСТОЙЧИВОГО РАЗВИТИЯ

ДЕЛОВАЯ ИГРА «МОДЕЛИРОВАНИЕ ГОРОДА КАК СЛОЖНОЙ САМООРГАНИЗУЮЩЕЙСЯ ЧЕЛОВЕКО-МАШИННОЙ СИСТЕМЫ»

Игнатьев Михаил Борисович
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, Большая Морская ул., 67
e-mail: ignatmb@mail.ru

Аннотация. Напротяжении многих лет автор использовал городка к объект моделирования при обучении студентов навыкам системного анализа и коллективной работы.Такой выбор объясняется тем,что город легко доступен для наблюдения и изучения,город является сложной самоорганизующейся системой,и его изучение позволяет проиллюстрировать многие принципы управления сложными системами.Эта деловая игра занимает целый семестри проводится с целым потоком студентов от 30 до 100 чел. Для управления большим коллективом разработчиков – студентов создается иерархическая система управления. Студенты открытым голосованием выбирают из своей среды руководителя города–мэра, который назначает своих заместителей по различным направлениям. В этом 2017 году мэром города была избрана Галина Зыкова, а ее заместителями – Леонид Артамонов и Валентин Елезов, которые представили обобщающий доклад.

Ключевые слова*: город как сложная система; моделирование; коллективная работа; умный город.*

BUSINESS GAME «MODELING CITIES AS COMPLEX SELF-ORGANIZING HUMAN-MACHINE SYSTEMS»

Ignatyev Mikhail
St. Petersburg state University of aerospace instrumentation
Russia, St. Petersburg, Bolshaya Morskaya str., 67
e-mail: ignatmb@mail.ru

Abstract. For many years the author used the city as an object of modeling in teaching students skills of system analysis and teamwork. This choice is due to the fact that the city is easily accessible for observation and study, the city is a complex self-organizing system, and its study allows to illustrate many of the principles of management of complex systems. This business game is a whole semester and is carried out with a flow of students from 30 to 100 people. To manage a large team of students creates a hierarchical control system. Students open ballot shall elect from its midst a head of the city mayor, who appoints his deputies in various areas. In this 2017, the mayor was elected Galina Zykova, and its Vice – Leonid Artamonov and Valentin Elesov, who provided a synthesis article.

Keywords: *the city as a complex system; modeling; teamwork; smart city.*

Условия игры следующие. Студентам предлагается придумать город, расположенный в любой точке земного шара и даже в космосе. В дискуссии студенты сочиняют легенду города, определяют его местоположение, численность населения, основные занятия жителей, придумывают название, герб и гимн. После этого каждый из студентов должен выбрать для разработки и анализа одну из подсистем города, например, поликлинику, торговый центр, полицейский участок, предприятие по производству компьютеров, транспортную контору, банк и т.д. [1, 2]. Каждый студент должен написать реферат по выбранной подсистеме города, который бы включал следующие части:

1) вербальное описание подсистемы и ее функционирования;

2) количественное описание подсистемы с определением количества занятых в подсистеме людей, технологий, финансовых потоков и др.;

3) разработку информационно-вы- числительной системы (ИВС), которая могла бы улучшить функци онирование подсистемы;

4) оценку эффективности разработанной ИВС и ее стоимости;

5) связь разработанной подсистемы с другими подсистемами города;

6) Элементы новизны.

При моделировании города как сложной системы были решены три задачи: во-первых, была осуществлена декомпозиция города на подсистемы; во-вторых, создана иерархическая система для управления проектом; в-третьих, студенческий коллектив осуществил разработку всех подсистем и их интеграцию в единое целое. Итогом этой работы являются, во-первых, рефераты каждого из студентов по выбранной подсистеме, увязанные с общегородскими проблемами, они начинают чувствовать свою миссию; во-вторых, определен сбалансированный бюджет города, что сделали мэр и его заместители по городу в целом, скоординировав работу отдельных студентов по подсистемам. В результате студенты получают навык в анализе и синтезе сложных систем и навык работы в коллективе. После этой деловой игры студенты выступают на конференции по информатике и проблемам устойчивого развития.

В этом 2017 году в качестве города для анализа был выбран Санкт-Петербург, перед жителями которого губернатор поставил задачу создать умный город. Некоторые из предложенных студентами идей стоит реализовать.

СПИСОК ЛИТЕРАТУРЫ

1. Игнатьев М.Б. «Кибернетическая картина мира. Сложные киберфизические системы» СПб, изд.ГУАП, с грифом УМО вузов России, 3-е издание, 2014, - 472 с.
2. Игнатьев М.Б. «Просто кибернетика» СПб, изд.Страта,2016, 250 с.

УДК 004.056

К ВОПРОСУ О СОЗДАНИИ НОВОГО ЗДАНИЯ МУЗЕЯ ОБОРОНЫ И БЛОКАДЫ ЛЕНИНГРАДА

Игнатьев Михаил Борисович[1], Макин Алексей Иванович[2], Мамошин Михаил Александрович[3], Никитин Александр Иванович[4], Фадеева Нина Владимировна[1]
[1]Региональная общественная организация воспитанников детских домов блокадного Ленинграда
Россия,Санкт-Петербург, Пушкинская ул., 5
[2]Музыкальное училище им. М.П. Мусорского
Россия,Санкт-Петербург, Моховая ул., 36
[3]Архитектурная мастерская Мамошина
Россия,Санкт-Петербург, наб. реки Мойки, 42
[4]Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, Большая Морская ул., 67
e-mail: ignatmb@mail.ru

Аннотация. Рассматривается проблема создания нового здания музея обороны и блокады Ленинграда с учетом прошлого опыта и перспектив применения новых технологий.

Ключевые слова: *история обороны Ленинграда; старый музей; виртуальная и дополненная реальности.*

THE QUESTION OF THE CREATION OF THE NEW BUILDING OF THE MUSEUM OF DEFENSE AND BLOCKADE OF LENINGRAD

Ignatyev Mikhail[1], Makin Alexey[2],Mimosin Michael[3], Nikitin Alexander[4], Fadeeva Nina[1]
[1]Regionalnaya public organization of pupils of orphanages in besieged Leningrad
Russia, St. Petersburg, Pushkinskaya str., 5
[2]Music School. M.P. Musorgsky
Russia, St. Petersburg, Mokhovaya St., 36
[3]Architectural workshop Mamoshin
Russia, St. Petersburg, nab. the Moika River, 42
[4]St. Petersburg State University of Aerospace Instrumentation
Russia, St. Petersburg, Bolshaya Morskaya str., 67
e-mail: ignatmb@mail.ru

Abstract. Deals with development of a new building of the Museum of defense and blockade of Leningrad on the basis of past experience and prospects of application of new technologies.

Keywords: *history of the defense of Leningrad; the old Museum; virtual and augmented reality.*

Вопросы информационной безопасности тесно связаны с патриотической воспитательной работой в обществе, что определяет мотивацию людей. В настоящее время развернулась острая борьба за трактовку исторических событий и в этом ряду героическая оборона и блокада Ленинграда в период 1941 – 1944 годов занимает особое значительное определившее победу место в ряду событий Второй мировой войны[1]. Музей обороны и блокады Ленинграда был организован в 1944 году после полного снятия блокады города, ему было выделено здание Всероссийской выставки народного хозяйства, построенное еще в царское время напротив Летнего сада площадью 40 тыс. квадратных метров. Этот музей пользовался большой популярностью среди жителей и гостей города, но в 1949 году в связи с так называемым Ленинградским делом музей был закрыт, а его сотрудники

репрессированы, и только в 1989 году по требованию общественности музей был вновь открыт, но в сильно урезанном виде, ему выделили лишь одну тысячу квадратных метров, что не соответствовало количеству накопленного материала и значению музея для города, страны и мира, и только в 2017 году было принято решение о строительстве нового здания музея в районе Смольного на берегу Невы. Это очень значимое место – ведь в Смольном помещался штаб обороны города. В сентябре 2017 года была открыта выставка проектов нового здания музея, было представлено девять проектов, среди которых выдающееся место занимал проект, подготовленный Архитектурной мастерской Мамошина, поэтому в нашем докладе он и рассматривается прежде всего.

По нашему мнению, проект Архитектурной мастерской Мамошина тоже нуждается в доработке. Это прежде всего создание лестницы памяти из 872 ступеней по числу дней блокады, для чего необходимо использовать подземное пространство. Преодоление лестницы памяти – лучшее средство для воспитания молодежи[1]. Во-вторых, создание светового конуса над зданием музей, для чего необходимо установить 12 прожекторов по кромке здания, лучи которых были бы направлены вверх под углом 75 градусов, управляя этими лучами можно было бы реализовать цветомузыку, соответствующую значимости тех событий. В-третьих, необходимо использовать технологии виртуальной и дополненной реальности для представления событий в действии. Разработка и реализация проекта нового здания музея обороны и блокады Ленинграда должна быть основана на предложениях ветеранов войны и жителей блокадного Ленинграда и явиться сама по себе важным актом патриотического воспитания.

СПИСОК ЛИТЕРАТУРЫ

1. Игнатьев М.Б. «Кибернетическая картина мира» СПб, изд. ГУАП, 2010.

УДК 004.896(08)

ОБ УПРАВЛЕНИИ РОБОТОТЕХНИЧЕСКИМИ СИСТЕМАМИ В ТРЕХМЕРНОМ ПРОСТРАНСТВЕ

Игнатьев Михаил Борисович[1], Катермина Татьяна Сергеевна[2], Липинский Ян Александрович[1], Ненашев Вадим Александрович[1]
[1]Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, ул. Большая Морская, 67
[2]Нижневартовский государственный университет
Нижневартовск, Ханты-Мансийский автономный округ,ул. Ленина, 56
e-mail: ignatmb@mail.ru

Аннотация. Рассматривается проблема управления роботами при перемещении в трехмерном пространстве на примере управления роботом для внутритрубной диагностики при перемещении вдоль оси трубы, на примере перемещения группы роботов по поверхности для управления группой умных автомобилей так, чтобы они не столкнулись в потоке машин, и на примере перемещения в трехмерном пространстве летающих роботов-беспилотников так, чтобы обеспечить безопасное перемещение группы летающих роботов.

Ключевые слова: *роботы для диагностики трубопроводов; внешнее управление умными автомобилями; внешнее управление беспилотниками; адаптация; безопасность в трехмерном пространстве.*

ABOUT THE CONTROL OF ROBOTIC SYSTEMS IN A THREE-DIMENSIONAL SPAC

Ignatyev Mikhail[1], Catermina Tatyana[2], Lipinski Jan[1],Nenashev Vadim[1]
[1]St. Petersburg State University of Aerospace Instrumentation
Russia, St. Petersburg, Bolshaya Morskaya str.,67
[2]Nizhnevartovskiy State University
Nizhnevartovsk, Khanty-Mansi Autonomous Area, Leninstr., 56
e-mail: ignatmb@mail.ru

Abstract. Considers the problem of robot control when moving in three-dimensional space on the example of robot control for in-line inspection when moving along the pipe axis, for example movement of a group of robots on the surface to manage a group of smart cars, so they do not run in traffic, and in the case of a three-dimensional movement of flying robots-drones to ensure safe movement of groups of flying robots.

Keywords: *robots for diagnostics of pipelines; external control smart cars; external control drones; adaptation; sefety in three-dimensional space.*

В качестве математической модели рассматривается кинематика материальной точки при перемещении по поверхности сферы, где Xi, Yi, Zi – координаты центра тяжести I - робота, а Ri – радиус сферы, по поверхности которого I - робот перемещается[1, 2]. Рассматривается перемещение как одиночного робота (I = 1), так и группы роботов (I = 1, 2, 3, 4, 5, 6 …). Если уравнение поверхности сферы

$$Xi2 + Yi2 + Zi2 - Ri2 = 0, \quad (1)$$

то после дифференцирования этого уравнения по времени и построения эквивалентных уравнений с произвольными коэффициентами [2], получим

$$\begin{aligned} dXi/dt &= U1^* Yi + U2^*Zi – U3^*Ri \\ dYi/dt &= - U1^*Xi + U4^*Zi – U5^*Ri \\ dZi/dt &= - U2^*Xi – U4^*Yi – U6^*Ri \\ dRi/dt &= - U3^*Xi – U5^*Yi – U6^*Zi \end{aligned} \quad (2)$$

где U1, U2, . . .,U6 – произвольные коэффициенты, которые могут быть использованы для управления перемещением i-робота, Xi, Yi, Zi – координаты i- робота при перемещении по сфере радиусом Ri. В частном случае при перемещении робота для внутритрубной диагностики по сфере с постоянным радиусом U3, U5, U6 эти произвольные коэффициенты можно положить равными нулю, а траекторию перемещения нашего робота задавать как пересечение сферы с плоскостью, что повышает безопасность.

$$A^*Xi + B^*Yi + C^*Zi = 0 \quad (3)$$

и структура уравнений (2) преобразуется к виду

$$\begin{aligned} dXi/dt &= U1^*(C^*Yi – B^*Zi) \\ dYi/dt &= - U1^*(C^*Xi – A^*Zi) \\ dZi/dt &= U1^*(B^*Xi – A^*Yi) \end{aligned} \quad (4)$$

где с помощью произвольного коэффициента U1 задается движение вперед или назад по диагностируемому газопроводу. Анализ этих уравнений приводит к построению простых цифровых автоматов, управляющих перемещениями робота для диагностики газопроводов.

Аналогичным образом строится система управления группой умных автомобилей в потоке машин так, чтобы они не столкнулись друг с другом путем установления оперативной радиосвязи между ними.

Также можно строить систему управления группой самолетов как пилотируемых людьми, так и беспилотников.

СПИСОК ЛИТЕРАТУРЫ

1. Игнатьев М.Б. «Голономные автоматические системы» изд. АН СССР, М-Л., 196, 202 с.
2. Игнатьев М.Б. «Кибернетическая картина мира. Сложные киберфизические системы» СПб, изд.ГУАП, 2014, 472 с.

УДК 100.32

ИНТЕНЦИОНАЛЬНЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ НА ОСНОВЕ ЛИНГВО-КОМБИНАТОРНОГО МОДЕЛИРОВАНИЯ

Игнатьев Михаил Борисович
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, Большая Морская ул., 67
e-mail: ignatmb@mail.ru

Аннотация. Как показывают исследования, в мозге память не имеет никаких ограничений или ячеек, каждое новое состояние перехода инициирует конструкцию локального шаблона, который внедряется и модифицирует всю интенциональную структуру. Показывается, что аналогичным образом действуют и структуры лингво-комбинаторного моделирования, предложенные автором еще в 1963 году.

Ключевые слова: *интенциональные структуры мозга; искусственный интеллект; лингво-комбинаторное моделирование; структурированная неопределенность.*

INTENTIONAL ARTIFICIAL INTELLIGENCE ON THE BASIS OF THE LINGUO-COMBINATORIAL SIMULATION

Ignatyev Mikhail
St. Petersburg state University of aerospace instrumentation
Russia, St. Petersburg, Bolshaya Morskaya str., 67
e-mail: ignatmb@mail.ru

Abstract. Studies show that brain memory has no limitations or cells, each new transition initiates a local design pattern that is implemented and modifies the whole intentional structure. It is shown that the same structure of linguo-combinatorial simulation, proposed by the author in 1963.

Keywords: *intentional structures of the brain; artificial intelligence; linguo-combinatorial simulation; structured uncertainty.*

В настоящее время наблюдается кризис в развитии систем искусственного интеллекта. Марвин Минский предложил фреймы – описания типичных ситуаций, когда создается список и используются только те факты, которые действительно релевантны. Но компьютеру сложно выбрать из множества

фреймов те фреймы, которые релевантны действительности. Важным шагом стали работы Фримана по когнитивной структуре мозга[2].

Но еще в 1963 году в моей книге [1] были рассмотрены структуры с произвольными коэффициентами, которые задавали поведение на пересечении многообразий и которые обладали свойствами контекстности и интенциальности. Далее они получили развитие в лингво-комбинаторном моделировании слабо формализованных систем[3], которые в настоящее время используются при управлении роботами, при моделировании организма для поддержки врачебных решений, при прогнозировании литосферной погоды и др. Выход из кризиса искусственного интеллекта лежит на пути создания интенционального интеллекта на основе лингво-комбинаторного моделирования.

СПИСОК ЛИТЕРАТУРЫ

1. Игнатьев М.Б. «Голономные автоматические системы», изд. АН СССР, 1963, - 202 с.
2. Freeman W. “Societies of Brains: A Study in the neuroscience of live and hate//Hillsdale, N.J.(ed.). The Spinoza Lecture, Amsterdam: Lawrence Erlbaum Associates, 1995.
3. Игнатьев М.Б. «Кибернетическая картина мира. Сложные киберфизические системы» СПб, изд.ГУАП, 3-е изд, 2014,-472 с.

УДК 621.374

МОДЕЛЬНОЕ ПРЕДСТАВЛЕНИЕ ИЗДЕЛИЙ ПРОГРАММИРУЕМОЙ ЛОГИКИ В ЗАДАЧАХ ОБРАТНОГО ПРОЕКТИРОВАНИЯ

Быков Андрей Владимирович, Демченко Олег Анатольевич, Усатый Вадим Анатольевич
Юго-Западный государственный университет
Россия, Курск, ул. 50 лет Октября,94
e-mails: andrey8310@inbox.ru, temp8@list.ru

Аннотация. Предложена формальная модель изделий программируемой логики, построенная на основе результатов анализа исполняемых модулей САПР, являющаяся основой методического, алгоритмического и программного обеспечения обратного проектирования.

Ключевые слова: *программируемая логика; обратное проектирование; модель.*

MODELREPRESENTATIONOFPROGRAMMABLE LOGIC DEVICES IN REVERSE ENGINEERING TASKS

Bykov Andrey, Demchenko Oleg, Usatiy Vadim
SWSU
Russia, Kursk, 50 years of October str.,94
e-mails: andrey8310@inbox.ru, temp8@list.ru

Abstract. A formal model of programmable logic devices, based on the results of CAD modules analysis, ispresent. This model is the basis of knowareand software.

Ключевые слова: *programmable logic; reverse engineering; model.*

Одним из перспективных направлений обеспечения информационной безопасности ответственных видов радиоэлектронной аппаратуры при применении в них элементной базы иностранного производства, а также при решении задач защиты интеллектуальной собственности является использование методов и технологий обратного проектирования.

В настоящее время наблюдается значительное увеличение применения изделий программируемой логики (ПЛ). Решение задачи выявления недокументированных возможностей зарубежного вычислительного оборудования в общем случае предполагает выполнение полного цикла работ по обратному проектированию электронных устройств, в том числе и реализованных на указанной элементной базе. Следует отметить, что с одной стороны обратное проектирование современных изделий ПЛ, являясь трудоемким процессом, требует значительных временных затрат и привлечения большого количества высококвалифицированных специалистов, а с другой в соответствии с [1] в настоящее время наблюдается тенденция отсутствия свободных средств для полномасштабного процесса обратного проектирования конфигурационных последовательностей таких изделий. В этой связи разработка и внедрение перспективных подходов к их обратному проектированию является актуальной и практически значимой научно-технической задачей.

В ряде работ [2, 3] предлагается подход к обратному проектированию на основе разработки как моделей ПЛ, так и моделей процесса обратного проектирования. В настоящее время основной математической моделью ПЛ является конечный структурный автомат с двоичным кодированием состояний, входных и выходных символов. Применительно к ПЛ автомат является инициальным и детерминированным, при этом процесс формирования автомата соответствует конфигурации ПЛ и полностью определяется конфигурирующей битовой последовательностью.

Вместе с тем, выбор автоматной модели для исследования характеристик какого-либо устройства может быть целесообразен в условиях отсутствия детальных знаний о его внутренней структуре и особенностях функционирования. Эта модель обеспечивает получение приемлемых

результатов только для относительно простых устройств (с ростом числа возможных состояний построение модели значительно усложняется). Наиболее существенный фактор, ограничивающий возможность практического применения данной модели, состоит в том, что в конфигурационных последовательностях ПЛ целого ряда фирм-производителей не содержится информации о связях между конфигурируемыми элементами, за исключением отдельных межсоединений. Для первых семейств ПЛ, содержащих десятки – сотни конфигурируемых блоков, такой подход позволял относительно достоверно (в среднем 95% связей восстанавливались правильно) определять правила формирования связей по отдельным межсоединениям. При этом разработка средств обратного проектирования для одного семейства ПЛ занимала достаточно длительное время. Отмеченные особенности существенно ограничивают возможность использования указанного подхода для обратного проектирования современных ПЛ в условиях априорной неопределенности знаний об алгоритмах формирования конфигурационных последовательностей, реализованных в САПР.

Таким образом, с учетом общих тенденций развития ПЛ, а именно с уменьшением технологических норм, увеличением логической плотности, повышением рабочих частот, интенсивным применением встраиваемых модулей, переходом от простых ПЛ к системам на кристалле, а также внедрением 3D транзисторных технологий актуальна задача разработки нового подхода к обратному проектированию ПЛ, в основе которого будет новая модель, учитывающая особенности внутренней структуры ПЛ и алгоритмы преобразования схемотехнической информации в конфигурационные последовательности. Поскольку фирмы-производители не раскрывают реализованные в их САПР алгоритмы формирования конфигурационных последовательностей и внутреннее представление ПЛ, а файлы САПР, содержащие информацию о ПЛ запакованы и в ряде случаев закодированы, то представляется, что единственным путем к получению необходимой информации является анализ исполняемых модулей САПР.

Методическая схема исследования при этом состоит из следующих этапов:

– восстановление внутреннего представления ПЛ, используемого компонентами САПР;

– восстановление алгоритмов генерации битовой загрузочной последовательности, реализованных в трансляторе и подключаемых библиотеках, при помощи анализа информации о внутреннем представлении ПЛ.

Анализ модулей САПР позволил установить, что внутреннему представлению ПЛ соответствует структура, представляющая собой двоичную матрицу, состоящая из блоков (двоичных подматриц), показанную на рисунке 1. Блоки соответствуют ресурсам ПЛ. При этом для каждого семейства ПЛ характерны свои типы ресурсов (блоков). Блоки одного типа имеют одинаковое внутреннее устройство.

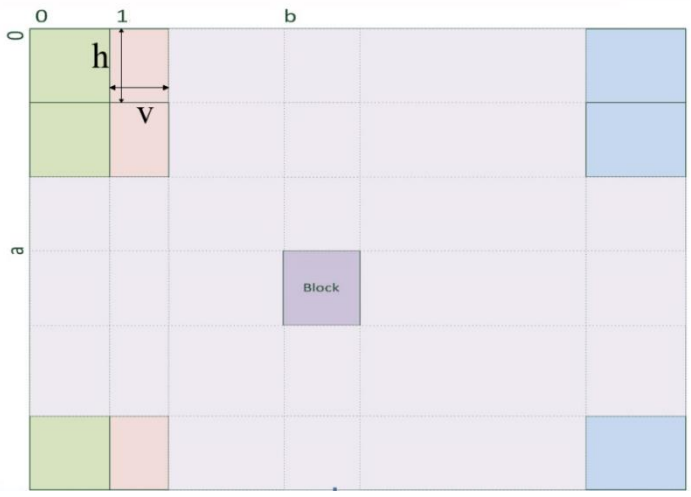


Рис.1. Внутреннее представление ПЛ в виде блоков.

На рисунке 1 использованы следующие обозначения: a – номер строки матрицы, содержащей левый верхний бит блока Block; b – номер столбца матрицы, содержащего левый верхний бит блока; h – высота блока (количество строк); v – ширина блока (количество столбцов). Каждый блок однозначно определяется соответствующими ему параметрами a, b, h и v.

Заполнение этой матрицы осуществляется последовательно – по блокам (подматрицам). В каждом блоке биты пронумерованы и каждому биту устанавливается значение в результате вычисления соответствующей ему двоичной формулы. При этом, в качестве операторов в этих формулах выступают следующие логические булевы функции: «и», «или» и «не». Для операндов могут быть восстановлены символьные, а в ряде случаев и индексные обозначения. Индексация осуществляется в рамках структуры, соответствующей типу блока, которому принадлежит данный бит.В результате проведенного анализа было восстановлено биективное преобразование указанной

матрицы в конфигурационную последовательность. При этом было установлено, что для каждого семейства ПЛ алгоритм этого преобразования уникален.

Таким образом, определены следующие особенности внутреннего представления ПЛ:

– внутреннее представление имеет блоковую структуру, при этом, все блоки можно классифицировать по типам;

– блоки одного типа имеют одинаковое устройство;

– значение каждого бита формируется в результате вычисления двоичной формулы.

С учетом отмеченных особенностей разработано модельное представление ПЛ, являющееся основой методического, алгоритмического и программного обеспечения обратного проектирования. Введены следующие обозначения:$B = (B_1, B_2, \dots, B_N)$– блоки ПЛ; $D_1, D_2, \dots, D_t$ – типы блоков; S – конфигурационная битовая последовательность; $F: B \to S$ – отображение, осуществляемое САПР.

В ходе анализа дизассемблированных модулей САПР установлено, что отображение F можно декомпозировать на композицию отображений $F = T \circ G$, где $T: B \to M$, M – двоичная матрица $T\begin{pmatrix} B_1 & \cdots & B_{i_1} \\ \vdots & \ddots & \vdots \\ B_{i_k} & \cdots & B_N \end{pmatrix} = \begin{pmatrix} T^1(B_1) & \cdots & T^{i_1}(B_{i_1}) \\ \vdots & \ddots & \vdots \\ T^{i_k}(B_{i_k}) & \cdots & T^N(B_N) \end{pmatrix} = \begin{pmatrix} M_1 & \cdots & M_{i_1} \\ \vdots & \ddots & \vdots \\ M_{i_k} & \cdots & M_N \end{pmatrix}$, $M_i = \begin{pmatrix} m_1^i & \cdots & m_a^i \\ \vdots & \ddots & \vdots \\ m_b^i & \cdots & m_h^i \end{pmatrix}$ – подматрица матрицы M $(m_q^i = \{0,1\})$, $G: M \to S$ – биективное преобразование. Каждый может быть описан состояниями его конфигурируемых элементов и программируемых межсоединений: $B_i = \{cfg^i, pip^i\}$, где $cfg^i = \{c_1^i, \dots, c_{l_i}^i\}$ – состояния конфигурируемыхэлементов, $c_j^i = \begin{cases} 0, \text{ не задействован} \\ 1, \text{задействован} \end{cases}$, $pip^i = \{p_1^i, \dots, p_{k_i}^i\}$ – состояния конфигурируемых межсоединений, $p_j^i = \begin{cases} 0, \text{ не задействовано} \\ 1, \text{ задействовано} \end{cases}$.

Каждый блок B_i имеет уникальное имя и относится к некоторому D_q.

Выполненный анализ модулей САПР позволил восстановить для каждого типа блоков D_q соответствующий набор ему двоичных формул, формирующих значения подматриц матрицы M: $t_1^q, \dots, t_p^q$, где $t_r^q: (cfg^q, pip^q) \to \{0,1\}$. Таким образом, если блок B_i имеет тип D_q, то $M_i = T^i(B_i) = T^{D_q}(B_i)$, а $m_v^i = t_v^q(cfg^q, pip^q)$ – результат вычисления соответствующей двоичной формулы.

Следовательно, для того чтобы определить задействованные элементы и активные межсоединения во всех блоках необходимо: 1) осуществить преобразование $G^{-1}: S \to M$; 2) для каждого блока B_i решить систему уравнений$\{m_v^i = t_v^q(cfg^q, pip^q)\}$.

В результате может быть получена структурная модель ПЛ, представленная на рисунке 2.

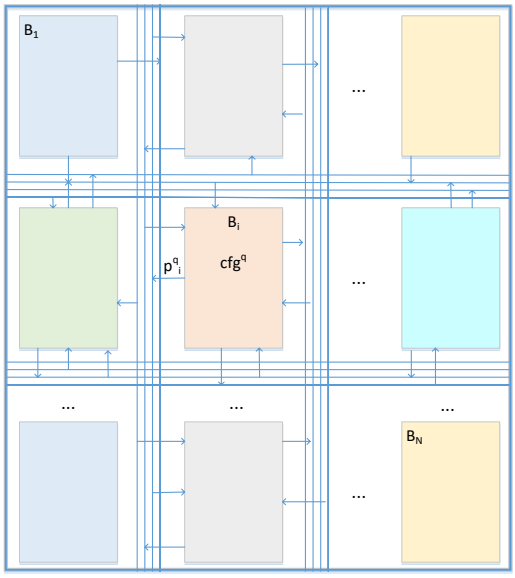


Рис. 2. Структурная модель ПЛ, восстановленная в результате обратного проектирования.

Построение такой модели может быть осуществлено в автоматическом режиме для каждой исследуемой конфигурационной последовательности. При этом определяется множество задействованных блоков и для каждого такого блока решаются системы двоичных уравнений. Анализ дизассемблированных модулей САПР позволил установить использование двоичной блоковой матрицы во внутреннем представлении всех исследованных семейств ПЛ.Следовательно, предложенная модель является универсальной. В ходе экспериментальных исследований установлено, что время, требуемое для построения такой модели, не превышало 1 мин. на типовой ЭВМ.

Следующий этап восстановления схемотехнической информации состоит в формировании связей между задействованными блоками, объединяя восстановленные в каждом блоке межсоединения в соответствии с правилами, восстановленными в ходе анализа САПР.

После успешного восстановления связей программными средствами обратного проектирования осуществляется преобразование восстановленной модели ПЛ в текстовый файл, содержащий схемотехническую информацию в формате, поддерживаемом САПР, который далее средствами САПР может быть преобразован вновь в конфигурационную последовательность для осуществления верификации (сравнения исходной и восстановленной конфигурационных последовательностей).

В ходе выполнения работ по обратному проектированию ПЛ определена структурно-функциональная организация комплекса программных средств обратного проектирования ПЛ, показанная на рисунке 3.

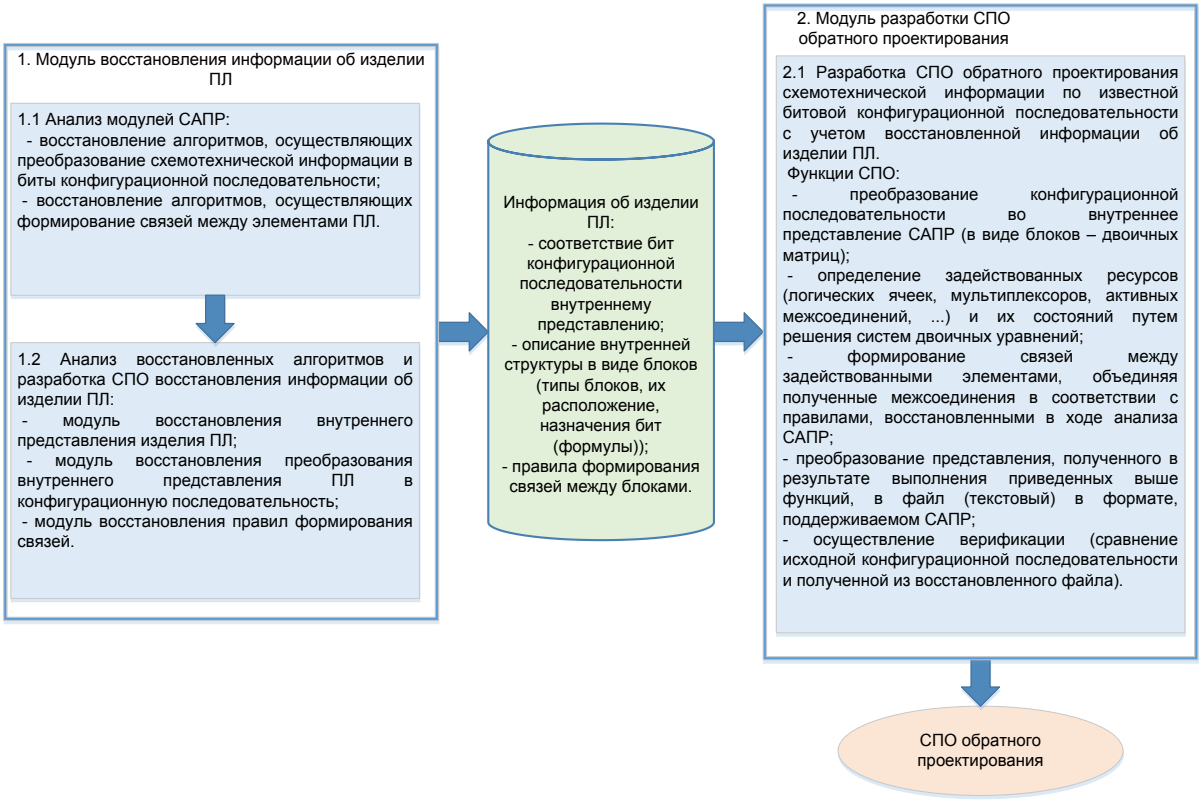


Рис. 3. Структурно-функциональная организация комплекса разработки программных средств обратного проектирования ПЛ.

Таким образом, на основе результатов анализа модулей САПР предложено универсальное модельное представление ПЛ, которое может быть положено в основу методического, алгоритмического и программного обеспечения обратного проектирования ПЛ.

СПИСОК ЛИТЕРАТУРЫ

1. Белов Е.Н., Балыбин С.В., Пономарев А.А., Семенов А.В., Федорец В.Н., Швыдя О.В. Перспективные технологии защиты микросхем от обратного проектирования в контексте информационной безопасности. Техносфера, Москва, 2017 –215 с.
2. Максфилд К. Проектирование на ПЛИС. Курс молодого бойца. – М.: Издательский дом «Додека-XXI», 2007. – 408 с.
3. Beckhoff C., Koch D., Torresen J., «Go ahead: a partial reconfiguration framework», 20th Annual IEEE Int. Symp. on Field-Programmable Custom Comp. Machines (April 29 – May 1, 2012, Toronto, Canada), 27–44.

УДК 004

СТРЕЛА ВРЕМЕНИ И НЕОБРАТИМОСТЬ ПРОЦЕССОВ В СЛОЖНЫХ ДИНАМИЧЕСКИХ СИСТЕМАХ

Острейковский Владислав Алексеевич[1], Муравьев Игорь Измайлович[2],
Шевченко Елена Николаевна[1]
[1]Сургутский государственный университет
Россия, ХМАО-Югра, Сургут, пр. Ленина, 1
[2] ПУ СургутАСУнефть
Россия, ХМАО-Югра, Сургут, ул.Энтузиастов, 50/1
e-mails: ostreykovsky_va@surgu.ru, igor_muraviov@mail.ru,elenan_27@mail.ru

Аннотация. Рассматриваются современные подходы к анализу фактора асимметрии времени в теории прогнозирования состояния сложных динамических систем.

Ключевые слова: *энтропия; необратимые процессы; асимметрия времени; модусы времени «прошлое-настоящее-будущее»; прогнозирование; стрела времени; время Ляпунова.*

THE TIME ARROW AND THE IRREVERSIBILITY OF PROCESSES IN COMPLEX DYNAMICAL SYSTEMS

Ostreykovsky Vladislav[1], Muraviov Igor[2],Shevchenko Elena[1]
[1]SurgutStateUniversity
Lenina str., 1, Surgut, Russia
[2] Open Joint Stock CompanySurgutneftegas
Entuziastov str. 50/1, Surgut, Russia
e-mails: ostreykovsky_va@surgu.ru, igor_muraviov@mail.ru,elenan_27@mail.ru

Abstract. Modern approaches to the analysis of the time asymmetry factor in the theory of forecasting the state of complex dynamical systems are considered.

Keywords: *entropy; irreversible processes; time asymmetry; time "past-present-future" modes; forecasting; arrow of time; the time of Lyapunov.*

Существуют две формулировки законов природы: Р.Клаузиуса и А.М.Ляпунова. Обе формулировки свидетельствуют о том, что: 1)существенным в описании состояния систем во времени являются необратимые процессы и 2)для сильно неустойчивых хаотических систем во времени наблюдается экспоненциальное разбегание траекторий. В обоих случаях имеет место стрела времени. Основная часть. Как известно, классическая динамика И.Ньютона описывает динамические процессы, в которых время $t \to +\infty$ и $t \to -\infty$ несущественно. Однако в природе имеют место случаи, когда именно направление времени имеет первостепенное значение. Изучением такого рода процессов исследователи начали интенсивно заниматься с конца XVIII в. В результате Р. Клаузиус в 1865 г. [1] сформулировал знаменитое второе начало термодинамики, в котором утверждал, что в некоторых процессах «односторонность» времени играет заметную роль. В понимании Р. Клаузиуса это характерно для изолированных систем, которые не обмениваются с внешним миром ни энергией, ни веществом, и для которых энтропия S монотонно возрастает до тех пор, пока не достигнет своего максимального значения в состоянии термодинамического равновесия

$$dS/dt \geq 0. \quad (1)$$

Затем было доказано, что выражение (1) обобщается и на системы, обменивающиеся энтропией и веществом с внешним миром. Таким образом, для открытых систем справедливо

$$dS = d_eS + d_iS, \quad (2)$$

где приращение энтропии d_eS описывает перенос энтропии через границы системы, d_iS – энтропию, произведенную в системе. Производство энтропии внутри системы согласно второму началу положительно. При такой формулировке стало понятным основное различие между обратимыми и необратимыми процессами. Такие необратимые процессы как диффузия, теплопроводность, химические реакции и другие дают вклад в производство энтропии. Из теории надежности известно, что интенсивность постепенных отказов $\lambda(t)$ для систем длительного использования растет во времени в связи с воздействием внешних и внутренних факторов, которые наиболее критичны при достижении объектом расчетного ресурса и срока службы для любых конструкционных материалов. Таким образом, наблюдается роль необратимых процессов (например, износа, коррозии, распада твердых растворов и т.п. процессов) в односторонности времени. Т.е. необратимые процессы влияют на положительное направление времени и постулируется существование функции с весьма специфическими свойствами. Эта функция может со временем только возрастать [2]!

Дальнейшие исследования в термодинамике необратимых процессов показали, что такие функции играют важную роль в современной теории устойчивости, заложенной в классических трудах А.М.Ляпунова [3]. Второе начало термодинамики позволяет утверждать, что для изолированных систем функция Ляпунова существует и термодинамическое равновесие является аттрактором для неравновесных состояний [4].М.Планк пошел еще дальше [5]. Он утверждал, что второе начало термодинамики позволяет выделять различные типы состояний в природе, из которых одни служат аттракторами для других. Т.е. необходимость есть не что иное, как проявление этой аттрактивности.

Таким образом, необратимые процессы играют одну из самых важных ролей в объяснении как стрелы времени, так и его асимметрии.

СПИСОК ЛИТЕРАТУРЫ

1. Клаузиус Р. О различных удобных для применения формах второго начала математической теории теплоты. -1865.
2. Антонов А.В., Острейковский В.А. Ресурс и срок службы оборудования энергоблоков атомных станций (на примере энергоблоков Смоленской АЭС): монография / А.В.Антонов, В.А.Острейковский. – М.: Инновационное машиностроение, 2017. – 536 с.
3. Ляпунов А. М. Собрание сочинений. М.; Л.: Изд-во АН СССР, 1954—1959
4. Пригожин И.Р. От существующего к возникающему. –М., «КомКнига», 2006. – 328 с.
5. Планк М. Картина мира современной физики // УФН – 1929. – Т. 9. – С. 407–436.

УДК 519.258

НЕПАРАМЕТРИЧЕСКИЕ МЕТОДЫ СТАТИСТИЧЕСКОГО АНАЛИЗА ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ

Погореловский Михаил Александрович, Григоренко Виолетта Вячеславовна, Назина Нина Борисовна, Заикин Павел Владимирович
Сургутский государственный университет
Россия, Сургут, ул. Ленина, 1
e-mails: pogorelovsky_ma@surgu.ru, grigv_84@mail.ru, nnb60@mail.ru, zaikinpv@gmail.com

Аннотация. В работе рассматриваются подходы к аппроксимации экспериментальных данных с помощью методов математической статистики. Обоснован выбор типа семейства кривых Пирсона для аппроксимации эмпирических данных. Произведены расчеты параметров основных типов уровнений для экспериментальных данных. Рассчитана адекватность применения кривых Пирсона с помощью критерия согласия Пирсона, χ^2 и критерия согласия Колмогорова-Смирнова.

Ключевые слова: *методы математической статистики; аппроксимация; кривые Пирсона; критерии согласия Колмогорова-Смирнова; критерий согласия Пирсона* χ^2*;*

NONPARAMETRIC METHODS OF STATISTICAL ANALYSIS OF EXPERIMENTAL DATA

Pogorelovsky Mikhail, Grigorenko Violetta, Nazina Nina, Zaikin Pavel
Surgut State University
Russia, Surgut, Lenin str., 1
e-mails: pogorelovsky_ma@surgu.ru, grigv_84@mail.ru, nnb60@mail.ru, zaikinpv@gmail.com

Abstract. This work examines the approaches to the approximation of the experimental data using the methods of mathematical statistics. The choice of the type of the family Pearson curves to approximate empirical data. Calculations curves of the main types of parameters for the experimental data. It calculated adequacy of Pearson curves using Pearson consent of fit, and the mark of the consent Kolmogorov-Smirnov.

Keywords: *methods of mathematical statistics; approximation; Pearson curves; Kolmogorov-Smirnov's consent; consent of fit Pearson* χ^2*.*

Исследователи в естественных и технических науках часто сталкивается спроцессами, поведения которых могут быть описаны с помощью методов математической статистики. Найденные закономерности имеют не только теоретическую ценность, они широко применяются на практике – в планировании, управлении и прогнозировании. Так же необходимо правильно подобрать метод статистического анализа и доказать целесообразность использования этого метода.

Первичная обработка экспериментальных данных необходима для дальнейшегопостроения моделей сложных систем. Так же необходимо определять законы распределения случайной величины.

Нахождение этого закона позволяет использовать полученные модели для прогнозирования и определения общих закономерностей.

Использование рядов Тейлора и Фурье затруднительно, т.к. они не обладают необходимыми свойствами: в начале и конце вариационного ряда, для которого строится функция плотности распределения, эта функция должна стремиться к нулю, а в середине ряда она должна достигать своего максимума. Иначе говоря, скорость изменения этой функции или выражающая эту скорость первая производная$\frac{dy}{dx}$ должна равняться нулю в трех точках: в начале и конце ряда, где $y = 0$, и в средине ряда, где функция достигает максимума.

Наиболее оптимальным вариантом, особенно в случае необходимости автоматической обработки значений, является использование универсальных семейств кривых. Таких как, например, семейство кривых Джонсона и семейство кривых Пирсона.Наиболее интересными, в смысле аппроксимации экспериментальных распределений, являются кривые Пирсона.

В данном эксперименте были использованы биомедицинские данные, полученные методами электрокардиографии и вариационной пульсографии. Информация о состоянии вариабельности сердечного ритма была получены с использованием пульсоксиметра, с помощью которого регистрируется пульсовая волна с одного из пальцев испытуемого в течении 5 минутного интервала времени. В качестве основного параметры использовались значения межимпульсных интервалов сердечных сокращений, которые показывают расстояния между ударами сердца.

Решение отдельного класса задач требует не только проверки соответствия распределения экспериментальных данных нормальному закону, но и определения к какому же закону распределения плотности вероятности относятся эти экспериментальные данные. Это задачи, связанные с распознаванием образов, задачи диагностики в медико-биологических системах, моделированием кинетики многокомпонентных смесей химико-технологических процессов нефтепереработки [3] и т.п.

Для определения закона распределения случайной величины необходимо:

1. Подобрать закона распределения;
2. Определить параметров функции плотности распределения;
3. Проверить адекватности выбора функции плотности распределения;

Рассмотрим подробно каждый из шагов.

Подбор вида распределения

Кривые Пирсона описываются дифференциальным уравнением:

$$dy/y = -\frac{x-M}{b_2x^2+b_1x+b_0}dx\ , \quad (1)$$

где началом отсчета x служит середина ряда, мода – M.

Дифференциальное уравнение (1) выражает общие свойства функций распределения. Постоянные коэффициенты, входящие в уравнение (1), можно выразить при помощи начальных и центральных моментов:

$$b_0 = \frac{4\beta_2-3\beta_1}{10\beta_2-12\beta_1-18}\mu_2\ , \quad (2)$$

$$b_1 = \frac{\sqrt{\mu_2}\sqrt{\beta_1}(\beta_2+3)}{10\beta_2-12\beta_1-18}, \quad (3)$$

$$b_2 = \frac{2\beta_2-3\beta_1-6}{10\beta_2-12\beta_1-18}\ , \quad (4)$$

где

$$\beta_1 = \frac{\mu_3^2}{\mu_2^3};\ \beta_2 = \frac{\mu_4}{\mu_2^2}\ , \quad (5)$$

а$\boldsymbol{\mu_2, \mu_3, \mu_4}$ соответственно центральные моменты 2, 3 и 4 порядков случайной величины x.

Вид функции плотности распределения определяется уравнением

$$b_2x^2 + b_1x + b_0 = 0, \quad (6)$$

Введем обозначение:

$$k = \frac{b_1^2}{4b_2b_0} \quad (7)$$

Обычнокоэффициент k называют каппой Пирсона. С учетом (2) и (3), запишем:

$$k = \frac{\beta_1(\beta_2+3)^2}{4(2\beta_2-3\beta_1-6)(4\beta_2-3\beta_1)} \quad (8)$$

Из формул (2-8) видно, что кривые Пирсона определяются при помощи первых четырех моментов.

Значениеk определяет тип кривой плотности распределения. В таблице 1 показаны значения k и соответствующие этим значениям кривые Пирсона [6].

Таблица 3.

Кривые Пирсона и соответствующие этим кривым уровнения, при заданных значения k

Значение k	Тип кривой Пирсона	Общий вид уравнения кривой
$k<0$	I	$y = y_0\left(1+\frac{x}{a_1}\right)^{m_1}\left(1-\frac{x}{a_2}\right)^{m_2}$
$0<k<1$	IV	$y = y_0\left(1+\frac{x^2}{a^2}\right)^{-m} \cdot e^{-\nu \arctan\frac{x}{a}}$
$k>1$	VI	$y = y_0(x-a)^{m_1}\cdot x^{-m_2}$
$k=0,$ $\mu_4=3$	Нормальное распределение	$y = \frac{1}{\sigma\sqrt{2\pi}}\cdot e^{-\frac{x^2}{2\sigma^2}}$
$k=0,$ $\mu_4<3$	II	$y = y_0\left(1-\frac{x^2}{a^2}\right)^{m}$
$k=0,$ $\mu_4>3$	VII	$y = y_0\left(1+\frac{x^2}{a^2}\right)^{-m}$
$k=1$	V	$y = y_0\cdot x^{-p}\cdot e^{-\frac{\gamma}{x}}$
$k=\pm\infty$	III	$y = y_0\left(1+\frac{x}{a}\right)^{\gamma a}\cdot e^{-\gamma x}$

где, y_0, a_i, γ, ν- параметры соответствующей кривой.

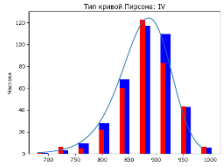
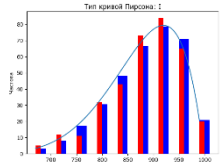
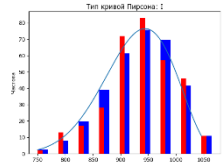
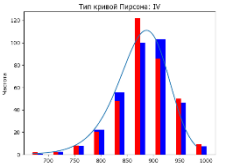
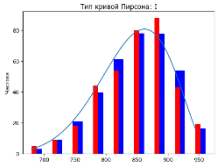
Алгоритм определение типа кривой Пирсона соответствующей эмпирическому распределению данных заключается в следующем[1]:

1. По статистическому ряду эмпирических данных определяют первые четыре момента распределения (начальный момент и центральные моменты).
2. Для целей нормирования, определяется разрядность ряда случайной величины с – т.е. среднюю длину отрезка между x_i, x_{i+1}.
3. Определяется медиана X_a случайной величины, как вариант, на котором достигается середина частотного ряда.
4. Вычисляется выравнивающий ряд, смещенный относительно центра ряда и нормированный согласно разрядности ряда. $x_i' = \frac{[(X]_i - X_a)}{c}$
5. Рассчитывается каппа Пирсона k.
6. Определяется тип кривой по классификации Пирсона.
7. Определяются параметры кривой плотности распределений. Для каждого из типов кривых существует уникальный порядок определения параметров. Каждый параметр вычисляется согласно ранее рассчитанных моментов, а также других характеристик случайной величины.

Для расчета подбора кривой распределения соответствующей эмпирическим данным была разработана компьютерная программа на языке Python [4]. В таблице 2 представлены результаты расчета 5 рядов статистических данных. Уравнения кривых составлены на основе значений статистических моментов, входящих в выражения соответствующей кривой. Рисунки иллюстрирую результаты аппроксимации эмпирических данных.

Таблица 2

Результаты расчета

№	график	Тип	уравнение	Критерий согласия Пирсона, χ^2	Критерий Колмогорова-Смирнова
1		IV	$y = 0.643 * \left(1 + \frac{x^2}{4.37^2}\right)^{-9.43} * e^{-11.5 * arcTan\left(\frac{x}{4.37}\right)}$	адекватность хорошая	адекватность хорошая
2		I	$y = 79.4 * \left(1 + \frac{x}{10.8}\right)^{5.26} * \left(1 - \frac{x}{1.97}\right)^{0.964}$	адекватность хорошая	адекватность хорошая
3		I	$y = 76.5 * \left(1 + \frac{x}{10.8}\right)^{9.91} * \left(1 - \frac{x}{4.07}\right)^{3.73}$	адекватность хорошая	адекватность хорошая
4		IV	$y = 0.754 * \left(1 + \frac{x^2}{4.28^2}\right)^{-8.84} * e^{-10.5 * arcTan\left(\frac{x}{4.28}\right)}$	адекватность хорошая	адекватность хорошая
5		I	$y = 80.8 * \left(1 + \frac{x}{10.5}\right)^{7.64} * \left(1 - \frac{x}{3.43}\right)^{2.49}$	адекватность хорошая	адекватность хорошая

Результат аппроксимирования кривыми Пирсона I и IV типа, эмпирических данных приведены в таблице 2, при этом проверка адекватности по 2 критериям, критерий χ^2 и Колмогорова-Смирнова

Всего было обработано 15 наборов исходных данных. Для доверительного интервала 0.05, 5 наборов данных вошли в доверительны интервал двух методов, 7 только у Колмогорова-Смирнова, а оставшиеся 3 – у критерия χ^2.

Вывод: таким образом можно считать, что семейство универсальных кривых типа Пирсона могут быть использовать для аппроксимации эмпирических биомедицинских данных.

СПИСОК ЛИТЕРАТУРЫ

1. Математическое моделирование ситуации возникновения критических состояний в организме человека [Журнал] / авт. Григоренко В.В. Лысенкова С.А., Гавриленко Т.В. // Вестник кибернетики. - -2015 -№2 (18) г.. - стр. -С 106-111.
2. Многомерный статистический анализ и временные ряды. / авт. Кендалл М. Стьюарт А. - М. : Наука, 2005.
3. Непрерывный подход в моделировании кинетики реакций многокомпонентной смеси / авт. Заикин П.В. Микшина В.С. // Вестник кибернетики. - 2014 г., - N1 г.. - стр. - с.25-31.
4. Программа визуализации кривыз семейства Пирсона [Патент] : № 2016613923 : свидетельство о гос. регистрации прогр. для ЭВМ / изобр. Погореловский Михаил Александрович и Заикин Павел Владимирович. - Российская Федерация, 15 февраль 2016 ..
5. Статистические модели в инженерных задачах / авт. Хан Г. Шапиро С. – М. : Мир, 1969. - стр. 400 с. - Пер. с англ..
6. Техника статистических вычислений. / авт. Митропольский А.К. - Москва : Наука, 1971. - стр. 570 с.

УДК 004.91

ПОДХОДЫ К ОЦЕНКЕ НАДЕЖНОСТИ СЛОЖНЫХ СИСТЕМ

Свеженцев Игорь Иванович
Смольный институт Российской академии образования
Россия, Санкт-Петербург, Полюстровский пр., 59
e-mail: sii6@rambler.ru.

Аннотация. Рассмотрены подходы к оценке надежности проектируемых сложных систем.

Ключевые слова: *надежность систем; проектирование; теория систем; сложные системы.*

APPROACHES TO ASSESSING THE RELIABILITY OF COMPLEX SYSTEMS

Svezhentsev Igor
Smolny Institute of the Russian Academy of Education
Russia, St. Petersburg, Polyustrovsky pr., 59
e-mail: sii6@rambler.ru.

Abstract. The approaches to the reliability assessment of the complexsystems being designed are considered.

Keywords: *reliability of systems; design; theory of systems; complex systems.*

Решению проблем проектирования сложных социально-экономических систем всегда уделялось пристальное внимание специалистов. По мере накопления опыта изменялись представления о системах и о путях и методах их проектирования.

Разработка принципиально нового подхода к решению проектных задач приводит к необходимости оценить уровень развития и методологический потенциал теории надежности, а также проблемы, находящиеся на стыке теории надежности, теории массового обслуживания и инженерной психологии.

Попытки дать обобщенное, целостное описание системы «человек - машина» зачастую связано с чрезвычайным упрощением, когда человек рассматривается как одно из звеньев системы. Требования проектировщиков, обращенные к психологам, сводятся к определению набора характеристик, которые следует приписать «человеческому компоненту». Традиционно указанные характеристики этого «компонента» описываются в иных понятиях (внимание, понимание задачи и др.), нежели машинного компонента. А в отношении человека в принципе нельзя построить модель, адекватную модели технического устройства; единственной истинной характеристикой человека является его изменчивость.

Разрешение этой проблемы на сегодняшний день производится на основе следующего постулата [1]. Поскольку в теории надежности единственными понятиями, описывающими функционирование системы, являются «выполнение» или «отказ», то роль человека должна быть записана только с помощью этих двоичных символов. При таком подходе, после проектирования на плоскость технического описания, от психологии остаются только конечные результаты:

- форма деятельности пользователя;
- операции, на которые разбивается деятельность;
- их взаимосвязь;
- внешние параметры выполнения операций (точность, время);

– параметры внутреннего состояния оператора и их влияние на внешние параметры (эмоциональное состояние, направленность).

Эти результаты объединяются с характеристиками технических устройств в общем цикле функционирования системы.

Таким образом, проектировщик системы получает возможность выбрать оптимальную последовательность операций, оценить потребную численность персонала для получения необходимых показателей функционирования систем, решить вопрос о номенклатуре специалистов.

Возвращение на определенном этапе развития научной теории к анализу ее основ вполне закономерно, если эта теория оправдывает себя в области практических приложений. Это относится к теории надежности. Вводившиеся при решении некоторых прикладных задач функционалы надежности, оказывались либо недостаточно универсальными, либо имели эвристический характер, что, безусловно, отражает трудности формализации их оценок [2, 3].

Строгое формулирование принципа надежности как одного из фундаментальных вариационных принципов проектирования, установление условий его единственности, позволит ввести в практику проектирования сложных систем критерий надежности, провести классификацию систем по надежности, обеспечить математический синтез оптимальных характеристик.

Конечной целью такой работы должна стать возможность решения широкого класса задач синтеза социально экономических систем ограниченной сложности на основе критерия обобщенной надежности, исследование задач синтеза характеристик надежных систем.

Важность и актуальность задач совершенствования теории надежности обусловлена тем, что указанный аспект – это неотъемлемая характеристика проектируемой системы. Любая корректная задача синтеза системы должна опираться на понятие системы данного уровня надежности.

Важное значение имеет также применение понятия надежности и к самому процессу проектирования (в виде надежности проектирования) и его автоматизации, так как оно непосредственно влияет на экономию времени и трудозатрат при создании систем, а также к формированию живучести и других существенных эксплуатационных характеристик систем.

Основные идеи математической теории систем связаны с понятиями состояния, управления, оптимизации и реализации [4].

Однако представляется необходимым присоединить к ним также понятие надежности социально - экономических систем, которое не только сочетает в себе различные грани указанных фундаментальных понятий, но и служит переходным мостом от теории к практике.

Следовательно, решение основных проектных задач может быть основано на обеспечении глубокой взаимосвязи теории надежности с концепцией проектирования. В этом случае появляется возможность трактовать систему проектирования, как систему управления движением в среде, роль которой играет целевое пространство проектирования. Подобная динамическая концепция предполагает, что теория надежности уже потенциально содержит в себе концепцию проектирования. С другой стороны, ее реализация должна с необходимостью базироваться на принципе надежности.

Представление о надежности социально-экономических систем, несомненно, является основополагающим для решения задач синтеза последних. Но это представление, на современном этапе, является скорее неформализованным описанием, чем строгим определением надежности (поскольку речь в нем идет о свойстве некоторого класса систем), и нуждается в соответствующей формализации. Недостаточная формализация исходных положений теории надежности уже сегодня может привести к трудностям при ее применении к новым классам систем и новым задачам проектирования.

В такой же степени принцип надежности охватывает, наряду с процессом проектирования системы в целом, и отдельные этапы ее проектирования.

Одним из главных результатов труда проектировщиков должен быть формализованный организационный порядок, который уменьшает неопределенность поведения управляемых объектов и оказывает существенное влияние на сам процесс и логику принятия решений, выступая в качестве ограничителя. При этом необходимо найти общую базу для взаимоотношений весьма специфических социальных, экономических и технических объектов.

Можно констатировать, что подходы и методики, разработанные и удовлетворявшие практику совершенствования в прошлом, в настоящее время все больше отстают от потребностей и новой проблематики современного уровня развития систем.

Для целей совершенствования и проектирования сложных систем на новых методологических основах должна быть разработана:

– концепция строения систем, включая структурно устойчивый каркас и организационную периферию, формирующую специфику;

– модель деятельности, построенная так, чтобы можно было ее применить к самым разным объектам проектирования.

Опираясь на концепции структуры и деятельности, должны применяться методы проектирования на основе совокупности производственной и управленческой технологий, взаимосвязано и целостно осуществляемых в любой сложной системе.

В ходе исследования проблемы обеспечения надежности сложных социально – экономических систем должно быть:

– уточнено и структурировано понятие «надежность сложных систем», а также группа сопутствующих понятий;

– исследована взаимосвязь надежности социально - экономической системы с процессом выполнения ею своей стратегической цели;

– для максимальной формализации принципа и критерия надежности для использования их в процессе проектирования подобран соответствующий математический аппарат;

– сформулированы и предложены методы и процедур управления надежностью социально - экономических систем на этапе их проектирования.

Установлено, что для обеспечения надежности, система должна не только иметь четко определенную цель, необходимые ресурсы и механизм их сбалансированного распределения в соответствии с целями, но и быть в состоянии адаптироваться к изменениям, как этого требуют быстрые изменения условий окружения.

СПИСОК ЛИТЕРАТУРЫ

1. Дэйвисон М. Многомерное шкалирование. - М.: Финансы и статистика, 1988. - 254 с.
2. Кандрашина Е.Ю., Литвинцева Л.В., Поспелов Д.А. Представление знаний о времени и пространстве в интеллектуальных системах /Под ред. Д.А. Поспелова. - Москва: Наука. - 1989. - 328 с.
3. Каплинский А.И., Руссман И.Б., Умывакин В.М. Моделирование и алгоритмизация слабоформализованных задач выбора наилучших вариантов систем. - Воронеж: Изд-во ВГУ, 1990. - 168 с.
4. Луценко Е.В. Автоматизированная система "ЭЙДОС" - как инструмент для разработки и эксплуатации психологических тестов //Теоретические и прикладные проблемы социально-психологической и медико-педагогической службы: Сб. науч. трудов. -Краснодар: КубГУ, 1995. - С.47-52.

ОГЛАВЛЕНИЕ

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В СФЕРЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 5

ИНФОРМАТИЗАЦИЯ НАЛОГОВОЙ СФЕРЫ В МОДЕЛИ ИДЕАЛЬНОГО ГОРОДА
Еремичев Даниил Андреевич 5

ПРОБЛЕМЫ ПОСТРОЕНИЯ СИТУАЦИОННЫХ ЦЕНТРОВ СУБЪЕКТОВ ФЕДЕРАЦИИ В УСЛОВИЯХ ПЕРЕХОДА К ЦИФРОВОЙ ЭКОНОМИКЕ
Жигадло Валентин Эдуардович 6

ПРОБЛЕМЫ УМНОГО ГОРОДА
Зыкова Галина Сергеевна, Артамонов Леонид Эдуардович, Елизов Валентин Олегович 13

МЕТОДОЛОГИЧЕСКИЕ И МЕТОДИЧЕСКИЕ ОСНОВЫ СОЗДАНИЯ И ПРИМЕНЕНИЯ КАТАСТРОФОУСТОЙЧИВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
Охтилев Михаил Юрьевич, Ключарев Александр Анатольевич, Соколов Борис Владимирович, Юсупов Рафаэль Мидхатович 15

НООСФЕРНОЕ ОБРАЗОВАНИЕ В РАЗВИТОМ ИНФОРМАЦИОННОМ ОБЩЕСТВЕ
Советов Борис Яковлевич 17

ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ КОСМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В ИНТЕРЕСАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИЙСКОЙ ФЕДЕРАЦИИ
Усатый Вадим Анатольевич, Ющенко Сергей Петрович 20

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ 24

ДИАГНОСТИРОВАНИЕ НАРУШЕНИЙБЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ
Авраменко Владимир Семенович, Маликов Альберт Валерьянович 24

ПРОГНОЗИРОВАНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ
Авраменко Владимир Семенович, Беденков Виктор Николаевич, Селяков Максим Николаевич 26

ОЦЕНКА РИСКОВ СЕТЕВОЙ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ НЕЧЕТКОГО ЛОГИЧЕСКОГО ВЫВОДА
Агеев Сергей Александрович,Саенко Игорь Борисович 28

СРЕДСТВА И СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ
Алашеев Вадим Викторович, Латушко Николай Александрович 30

РАЗВЕРТЫВАНИЕ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ ДИСТАНЦИОННОГО ОБУЧЕНИЯ В СУЩЕСТВУЮЩЕЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ
Алексеев Олег Владимирович, Ногин Сергей Борисович, Чесноков Александр Валерьевич 32

ВНЕДРЕНИЕ СЕРВИСА «ИНФРАСТРУКТУРА КАК СЕРВИС» ДЛЯ ПРОВЕДЕНИЯ КОМПЛЕКСНЫХ ПРАКТИЧЕСКИХ ЗАНЯТИЙ С ДОЛЖНОСТНЫМИ ЛИЦАМИ ОРГАНА УПРАВЛЕНИЯ
Алексеев Олег Владимирович, Ногин Сергей Борисович, Чесноков Александр Валерьевич 33

ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ СВЯЗЬЮ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
Башкирцев Андрей Сергеевич 34

ОРГАНИЗАЦИЯ РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ РАЗНОРОДНЫХ СРЕДСТВ АВТОМАТИЗАЦИИ
Башкирцев Андрей Сергеевич, Зибров Олег Павлович
Зобнин Константин Александрович, Усачёв Игорь Владимирович 36

МЕЖСЕТЕВЫЕ ЭКРАНЫ КАК ЭЛЕМЕНТ АРХИТЕКТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИСИСТЕМ УПРАВЛЕНИЯ СОВРЕМЕННЫМИ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ И ЦЕНТРАМИ ОБРАБОТКИ ДАННЫХ
Башкирцев Андрей Сергеевич, Михайличенко Николай Валерьевич, Паращук Игорь Борисович 37

ВОПРОСЫ МОДЕЛИРОВАНИЯ СОВРЕМЕННЫХ СИСТЕМ СВЯЗИ
Беззубов Олег Владимирович 39

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
Безуглый Юрий Андреевич, Вершенник Алексей Васильевич 41

ЗАЩИТА САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ УКВ ДИАПАЗОНА СИЛОВЫХ СТРУКТУР
Бесков Андрей Владимирович, Вотинов Михаил Леонардович, Ковайкин Юрий Владимирович, Кривошей Ольга Ивановна 43

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕПРЕДЛОЖЕНИЯ ПО ПОВЫШЕНИЮ ЗАЩИЩЕННОСТИ ЛВСОТ КОМПЬЮТЕРНОЙ РАЗВЕДКИ
Бесков Андрей Владимирович, Кирьянов Александр Сергеевич, Ковайкин Юрий Владимирович, Наджафов Гаджи Амамдинович, Уйманов Андрей Викторович 45

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСКРЕЦИОННОЙ МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ СРЕДСТВАМИ РОЛЕВОЙ МОДЕЛИ
Бирюков Михаил Александрович, Волкова Евгения Валерьевна, Саенко Игорь Борисович 46

СПОСОБ РЕАЛИЗАЦИИ МАНДАТНОЙ МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ РОЛЕВОЙ МОДЕЛИ
Бирюков Михаил Александрович, Зибров Олег Павлович, Саенко Игорь Борисович 48

ОРГАНИЗАЦИЯ ЗАЩИЩЁННЫХ ПРОЦЕССОВ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ
Борец Дмитрий Владимирович, Ковалев Игорь Станиславович, Малышев Виктор Сергеевич, Пантюхин Олег Игоревич 50

ОЦЕНКА ОПЕРАТИВНОСТИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПУНКТА УПРАВЛЕНИЯ СИЛОВОГО ВЕДОМСТВА
Борец Дмитрий Владимирович, Ковалев Игорь Станиславович, Малышев Виктор Сергеевич, Пантюхин Олег Игоревич 52

ТЕХНИЧЕСКИЕ СРЕДСТВА ПОРАЖЕНИЯ ИНФОРМАЦИОННЫХ КОМПЛЕКСОВ
Борисов Алексей Александрович, Владимиров Дмитрий Радиевич 54

АНАЛИЗ ПРОБЛЕМ РАЗВИТИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
Борисов Александр Иванович, Логинов Вячеслав Алексеевич, Пименов Алексей Сергеевич 54

ХРОНОЛОГИЧЕСКИЕ ПРИЗНАКИ ЗАЩИЩЕННОСТИ СЕТИ СВЯЗИ И ЕЁ ЭЛЕМЕНТОВ ОТ КОМПЬЮТЕРНЫХ АТАК
Бречко Александр Александрович, Львова Наталия Владиславовна, Латушко Николай Александрович 56

ОБЗОР МЕТОДОВ ШИФРОВАНИЯ
Буханов Павел Юрьевич, Смирнов Дмитрий Михайлович, Хан Георгий Георгиевич, Бирюков Михаил Александрович 58

ФУНКЦИОНАЛЬНО-ДИСКРЕЦИОННАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ
Валюшкина Юлия Андреевна 60

ПОДХОД К ПРОТИВОДЕЙСТВИЮ КОМПЬЮТЕРНЫМ АТАКАМ НАКРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СЕГМЕНТАХ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
Васюков Дмитрий Юрьевич, Смыгин Александр Михайлович Митрофанов Михаил Валерьевич 61

БЕЗОПАСНОСТЬ — ПРОБЛЕМА ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА
Вертепов Михаил Васильевич, Букреев Денис Дмитриевич, Гавриленко Владимир Андреевич 63

СПОСОБ ЗАЩИТЫ АБОНЕНТСКИХ ЛИНИЙ
Вершенник Алексей Васильевич, Вершенник Елена Валерьевна, Куприянов Никита Алексеевич, Стародубцев Юрий Иванович 64

КОНЦЕПТУАЛЬНЫЕ ПОДХОДЫ К ПРОБЛЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЛЕКСОВ С БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ
Винокуров Александр Владимирович, Лозовский Владимир Валерьевич, Кибенко Александр Викторович 66

ЗАЩИТА МИКРОПРОЦЕССОРНЫХ СРЕДСТВ ОБРАБОТКИ ДАННЫХ ОТ ПРЕДНАМЕРЕННЫХ СИЛОВЫХ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЙ
Владимиров Дмитрий Радиевич, Борисов Алексей Александрович 68

О СПОСОБАХ МОДЕЛИРОВАНИЯ СЕТЕЙ СВЯЗИ
Волкова Евгения Валерьевна, Чукариков Александр Геннадьевич 69

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ПЕРЕДАЧИ, ХРАНЕНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ
Волостных Виктор Анатольевич, Рогов Руслан Александрович, Митрофанов Михаил Валерьевич 71

О НЕКОТОРЫХ МЕТОДАХ СЕТЕВОГО АНАЛИЗА
Гапочкин Артем Владимирович, Михайличенко Николай Валерьевич 72

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК
Гладков Владимир Владиславович, Тараскина Анастасия Геннадьевна,
Кузнецов Сергей Иванович, Тесля Сергей Петрович, Акишин Андрей Владимирович 73

ВОПРОСЫ ПЛАНИРОВАНИЯ МЕРОПРИЯТИЙ ОПЕРАТИВНО-ТЕХНИЧЕСКОЙ СЛУЖБЫ НА ОБЪЕКТАХ АВТОМАТИЗАЦИИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
Григорян Вазген Мкртичевич, Куликов Владимир Алексеевич
Пантюхин Олег Игоревич, Солодухин Борис Владимирович 75

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПОД УПРАВЛЕНИЕМ ОПЕРАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ASTRA LINUX SE
Гринь Дарья Владимировна, Ильина Ольга Борисовна, Купчиненко Ольга Павловна,
Скоропад Александр Витальевич 76

К ВОПРОСУ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПЛАНИРОВАНИЯ ПОВСЕДНЕВНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНА УПРАВЛЕНИЯ
Гурьев Сергей Николаевич, Щербаков Александр Юрьевич 78

АБСОЛЮТНО СТОЙКОЕ КВАНТОВОЕ ШИФРОВАНИЕ
Гущин Игорь Николаевич, Петренко Михаил Игоревич, Овчинников Николай Юрьевич 79

НЕКОТОРЫЕ ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ВЗАИМОДЕЙСТВИИ РЕГИОНАЛЬНЫХ КОРПОРАТИВНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ С СЕТЬЮ ОБЩЕГО ПОЛЬЗОВАНИЯ
Дедюрин Антон Борисович, Еричев Павел Сергеевич, Паращук Игорь Борисович 81

ТИПЫ СРЕДСТВ ДОВЕРЕННОЙ ЗАГРУЗКИ И ИХ РОЛЬ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ
Жмуров Владислав Дмитриевич, Паращук Игорь Борисович, Саяркин Леонид Андреевич 82

СПОСОБ ЗАЩИТЫ РЕСУРСОВ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ
Журавель Евгений Павлович 84

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ С ПРИМЕНЕНИЕМ НЕЙРОННЫХ СЕТЕЙ
Захаров Руслан Владимирович, Лаута Олег Сергеевич, Крибель Александр Михайлович,
Дмитрий Владимирович Соловьев 92

АНАЛИЗ ТЕНДЕНЦИЙ ПРИМЕНЕНИЯ И ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ ХРАНЕНИЯ ДАННЫХ ДЛЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ
Зияев Павел Викторович, Паращук Игорь Борисович, Ткаченко Владимир Владиславович 93

МЕТОД ИЗМЕРЕНИЯ ПАРАМЕТРОВ ИОНОСФЕРЫ ДЛЯ ОЦЕНКИ СВОЙСТВ И ХАРАКТЕРИСТИК СПУТНИКОВОЙ РАДИОСВЯЗИ
Зорин Владимир Андреевич, Корякин Денис Дмитриевич, Андреев Глеб Владимирович 95

АСПЕКТЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИИVPN В КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУРАХ
Зубакин Владимир Валентинович, Кий Андрей Вячеславович, Морозов Иван Васильевич 97

ПОСТАНОВКА ЗАДАЧИ НАХОЖДЕНИЯ МЕСТОРАСПОЛОЖЕНИЯ КОНТРОЛЛЕРА НА ПРОГРАММНО-КОНФИГУРИРУЕМОЙ СЕТИ
Зубакин Владимир Валентинович, Хмелляр Николай Александрович,
Шинкарев Семен Александрович 99

МОДЕЛЬ НАРУШИТЕЛЯ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ АБДУКТИВНОГО СИНТЕЗА СТРУКТУР СЦЕНАРИЕВ
Карганов Виталий Вячеславович, Липатников Валерий Алексеевич 100

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ
Карпов Александр Владимирович 102

ПОДХОДЫ К СОВЕРШЕНСТВОВАНИЮ СИСТЕМЫ КОНТРОЛЯ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТЕ УПРАВЛЕНИЯ
Карпов Александр Владимирович, Лепешкин Олег Михайлович 103

МЕТОДИКА ПРОГНОЗИРОВАНИЯ ПРОТОКОЛЬНЫХ ВОЗДЕЙСТВИЙ НА РОБОТИЗИРОВАННЫЕ СИСТЕМЫ
Коцыняк Михаил Антонович, Дементьев Владислав Евгеньевич, Тесля Сергей Петрович, Лаута Олег Сергеевич 105

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕТЕЙ СТАНДАРТА IEEE 802.11
Колнооченко Анастасия Александровна 107

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА КАНАЛА УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ
Коцыняк Михаил Антонович, Гудков Михаил Александрович, Сафонов Алексей Александрович, Борис Артурович Арутюнян 108

МЕТОДИКА ПРОГНОЗИРОВАНИЯ ВОЗДЕЙСТВИЯ ТАРГЕТИРОВАННОЙ КИБЕРНЕТИЧЕСКОЙ АТАКИ НА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННУЮ СЕТЬ
Коцыняк Михаил Антонович, Иванов Денис Александрович, Лаута Олег Сергеевич, Нечепуренко Александр Петрович, Муртазин Ильдар Робертович 109

ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Киреев Сергей Хаирбекович 111

ПРОБЛЕМА ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОГО СОПРЯЖЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ РАЗЛИЧНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
Кондрашов Юрий Владимирович, Максименко Евгений Алексеевич 113

МЕТОДИКА ОЦЕНКИ КОМПЛЕКСНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ИТКС СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
Коцыняк Михаил Антонович, Ястребов Владимир Васильевич, Клиншов Илья Андреевич, Гулевич Антон Владимирович 114

ЗАЩИТА ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННЫМ КАНАЛАМ СВЯЗИ ПОЧТОВЫХ СЕРВЕРОВ
Крибель Александр Михайлович, Корякин Денис Дмитриевич 115

ВЕРОЯТНОСТНО-ВРЕМЕННЫЕ ХАРАКТЕРИСТИКИ АТАК НА РОБОТИЗИРОВАННЫЕ СИСТЕМЫ
Кузнецов Сергей Иванович, Иванов Денис Александрович, Власенко Максим Андреевич, Латушко Николай Александрович 117

УСТОЙЧИВОСТЬ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ В УСЛОВИЯХ КОМПЬЮТЕРНЫХ АТАК
Кузнецов Сергей Иванович, Новиков Павел Аркадьевич, Кузнецова Анастасия Алексеевна 118

СПОСОБ УМЕНЬШЕНИЯ СЛУЖЕБНОГО ТРАФИКА В СЕТИ ПЕРЕДАЧИ ДАННЫХ С КОММУТАЦИЕЙ ПАКЕТОВ
Курашев Заур Валерьевич 119

ПОДХОД К ОЦЕНКЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ОТ ТЕХНИЧЕСКОЙ КОМПЬЮТЕРНОЙ РАЗВЕДКИ
Лаута Олег Сергеевич, Клиншов Илья Андреевич, Ястребов Владимир Васильевич, Русаков Егор Владимирович 121

ПРОБЛЕМЫ И ПУТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СПУТНИКОВОЙ СВЯЗИ
Лебеда Евгений Вячеславович, Тарасов Александр Сергеевич 123

РАЗРАБОТКА НАУЧНО-МЕТОДИЧЕСКОГО АППАРАТА ИДЕНТИФИКАЦИИ И ПРОГНОЗИРОВАНИЯ ЭВОЛЮЦИИ МЕЖЭТНИЧЕСКИХ И МЕЖКОНФЕССИОНАЛЬНЫХ КОНФЛИКТОВ, ВОЗНИКАЮЩИХ В РЕЗУЛЬТАТЕ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА
Лозовский Владимир Валерьевич, Винокуров Александр Владимирович, Галицкий Валерий Андреевич 125

АНАЛИЗ СПОСОБОВ МОДЕЛИРОВАНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ В КИБЕРПРОСТРАНСТВЕ
Львова Наталия Владиславовна, Бречко Александр Александрович, Баленко Ольга Александровна 127

ИСПОЛЬЗОВАНИЕ ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ КОНТРОЛЛЕРОВ ДЛЯ ИЗМЕРЕНИЯ ПАРАМЕТРОВ НАПРЯЖЕНИЯ В СЕТЯХ ЭЛЕКТРОСНАБЖЕНИЯ
Мель Михаил Игоревич, Щукин Андрей Владимирович 129

ВОПРОСЫ ЗАЩИТЫ ИНТЕРЕСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ
Неижмак Алексей Владимирович 130

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА
Мехряков Александр Владимирович, Шибанов Данил Сергеевич, Трифонов Павел Валерьевич, Бирюков Михаил Александрович 132

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА ОСНОВЕ ВЫБОРА ЗАЩИЩЕННЫХ ИНТЕРВАЛОВ СВЯЗИ ОТ РАДИОПОДАВЛЕНИЯ
Митрофанов Михаил Валерьевич., Ракицкий Станислав Николаевич, Чиков Дмитрий Викторович 134

ИССЛЕДОВАНИЕ ПРОЕКТИРОВАНИЯ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ
Михайлов Вячеслав Викторович, Ильичёв Святослав Игоревич, Федосеев Денис Олегович, Степанова Елена Александровна 135

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ
Михайличенко Николай Валерьевич 137

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МОБИЛЬНЫХ УСТРОЙСТВАХ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ
Неижмак Алексей Владимирович 139

ИССЛЕДОВАНИЕ ПРОБЛЕМЫ ПРОСЛУШИВАНИЯ СЕТЕВОГО ТРАФИКА
Нехань Евгений Николаевич, Гудков Михаил Александрович 140

К ВОПРОСУ ФУНКЦИОНАЛЬНОГО, ОРГАНИЗАЦИОННОГО И СТРУКТУРНОГО ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ВЗАИМОДЕЙСТВИИ РЕГИОНАЛЬНЫХ КОРПОРАТИВНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ С СЕТЬЮ ОБЩЕГО ПОЛЬЗОВАНИЯ
Нехань Евгений Николаевич, Паращук Игорь Борисович, Скрябин Евгений Андреевич 142

МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНЫХ ВОЗДЕЙСТВИЙ
НечепуренкоАлександр Петрович, Суетин Артем Игоревич, Муртазин Ильдар Робертович, Лаута Олег Сергеевич 144

МОДЕЛИРОВАНИЕ ТЕРРИТОРИАЛЬНОГО РАСПРЕДЕЛЕНИЯ БАЗОВЫХ СТАНЦИЙ СЕТЕЙ ШИРОКОПОЛОСНОГО РАДИОДОСТУПА
Овсянников Станислав Николаевич, Панин Роман Сергеевич, Калюка Владимир Иванович 145

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ БЕСПРОВОДНОГО АБОНЕНТСКОГО ДОСТУПА
Овсянников Станислав Николаевич, Панин Роман Сергеевич, Калюка Владимир Иванович 147

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ДЕМОДУЛЯЦИИ СИГНАЛОВ
Овчинников Николай Юрьевич, Петренко Михаил Игоревич 149

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННОЙ КОМПОНЕНТЫ КИБЕРФИЗИЧЕСКИХ СИСТЕМ
Паращук Игорь Борисович 150

ПРОБЛЕМАТИКА ПЛАНИРОВАНИЯ ПРИМЕНЕНИЯ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
Пименов Алексей Сергеевич, Деньжонков Кирилл Александрович
Борисов Александр Иванович, Прудников Евгений Константинович 152

ПРИНЦИПЫ МОДЕЛИРОВАНИЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ, ВКЛЮЧАЮЩИХ РАДИОСЕТИ С ПАКЕТНОЙ ПЕРЕДАЧЕЙ ДАННЫХ
Попов Андрей Иванович, Михайличенко Николай Валерьевич 154

МЕТОД РАНДОМИЗИРОВАННЫХ СВОДНЫХ ПОКАЗАТЕЛЕЙ ДЛЯ ЭКСПЕРТНОЙ ОЦЕНКИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ
Попова Елена Владимировна 155

ВЫБОР МЕТОДА ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ ДЛЯ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ
Прудников Евгений Константинович, Пименов Алексей Сергеевич, Ащеулов Сергей Викторович 158

АНАЛИЗ ПРОБЛЕМЫ КОНТРОЛЯ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ
Саенко Игорь Борисович 159

РАЗРАБОТКА МЕТОДА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ВЫБОРУ АППАРАТНО-ПРОГРАММНЫХ МОДУЛЕЙ ДОВЕРЕННОЙ ЗАГРУЗКИ В ИНТЕРЕСАХ ЗАЩИТЫ ОТ НСД НА АРМ ДОЛЖНОСТНЫХ ЛИЦ СИЛОВЫХ ВЕДОМСТВ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ
Саяркин Леонид Андреевич 161

ОБЪЕДИНЕННАЯ АРХИТЕКТУРА БЕЗОПАСНОСТИ ДЛЯ ЗАЩИТЫ КОРПОРАТИВНОЙ СЕТИ
Селяков Максим Николаевич, Пащенко Василий Владимирович,
Беденков Виктор Николаевич, Матвеев Александр Николаевич 162

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В ПРИЛОЖЕНИЯХ НА ПЛАТФОРМЕ ASP.NET
Скрябин Евгений Андреевич, Зайцев Данила Евгеньевич 164

О ПРОБЛЕМЕУПРАВЛЕНИЯ ВИРТУАЛЬНЫМИ ЛОКАЛЬНЫМИ ВЫЧИСЛИТЕЛЬНЫМИ СЕТЯМИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ
Старков Артем Михайлович, Саенко Игорь Борисович 166

АНАЛИЗ НАЗНАЧЕНИЯ ОСНОВНЫХ ФУНКЦИЙ, РЕАЛИЗУЕМЫХ В ПРОЦЕССЕ УПРАВЛЕНИЯ УС СН
Сутырин Вячеслав Геннадьевич, Хмелевской Валерий Павлович 168

ТРЕБОВАНИЯ К ВОЗМОЖНАСТЯМ ФУНКЦИИ «УЧЕТ», РЕАЛИЗУЕМОЙ ПРИ ОРГАНИЗАЦИИ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ УЗЛОМ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
Сутырин Вячеслав Геннадьевич, Хмелевской Валерий Павлович 169

ПОДХОД К ПОСТРОЕНИЮ ИМИТАЦИОННОЙ МОДЕЛИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОБОТОТЕХНИЧЕСКОГО КОМПЛЕКСА
Теплов Иван Андреевич, Махнач Андрей Валерьевич, Саенко Игорь Борисович 171

ПОДХОД К ОБОСНОВАНИЮ ТРЕБОВАНИЙ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ
Тесля Сергей Петрович, Мартынюк Иван Анатольевич, Федорова Светлана Владимировна,
Чоп Алексей Андреевич 172

ОБЕСПЕЧЕНИЕИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ ХРАНЕНИЯ ДАННЫХ
Ткаченко Владимир Владиславович 174

БЕЗОПАСНОСТЬ В СЕТЯХ МОБИЛЬНОЙ СВЯЗИ. ЗАЩИТА ИНФОРМАЦИОННЫХ РЕСУРСОВ В СЕТЯХ 4G
Ульянов Максим Владимирович, Годунов Евгений Романович, Терехов Александр Геннадьевич 175

К ВОПРОСУ О ПРОБЛЕМЕ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
Усачев Игорь Владимирович, Кий Андрей Вячеславович, Зибров Олег Павлович,
Башкирцев Андрей Сергеевич, Щербаков Александр Юрьевич 177

ПРОГРАММНАЯ СИСТЕМА ДЛЯ МОНИТОРИНГА СЕТЕВОГО ОБОРУДОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Федосеев Денис Олегович, Корякин Денис Дмитриевич, Ястребов Егор Евгеньевич 179

МЕТОДИКА ПРОЕКТИРОВАНИЯ СИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
Фиалкин Илья Александрович 181

АНАЛИЗ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ХЕШ-ФУНКЦИЙ ДЛЯ СРАВНЕНИЯ ТЕКСТОВ БЕЗ РАСКРЫТИЯ СОДЕРЖИМОГО
Хилько Валерий Олегович, Левкин Александр Сергеевич 182

ПОИСК ДУБЛИКАТОВ В ИСХОДНЫХ КОДАХ ПРОГРАММ
Хилько Валерий Олегович, Шаров Илья Александрович 184

МОДЕЛЬ ДЛЯ ОПРЕДЕЛЕНИЯ СКРЫТНОСТИ СИСТЕМЫ СВЯЗИ
Худайназаров Юрий Кахрамонович, Маслов Олег Николаевич, Барауля Игорь Геннадьевич 185

НЕОБХОДИМОСТЬ РАЗРАБОТКИ СИСТЕМЫ ТРЕБОВАНИЙ К ОПЕРАЦИОННЫМ СИСТЕМАМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
Чесноков Александр Валерьевич, Юдин Анатолий Алексеевич, Алексеев Олег Владимирович 187

ПРОГРАММА ДЛЯ МОДЕЛИРОВАНИЯ ОБЪЕКТОВ – SKETCHUP
Шибанов Данил Сергеевич 189

АКТУАЛЬНОСТЬ РАЗВИТИЯ СЕТЕВОГО КОНТРОЛЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ
Шостак Роман Константинович, Лепешкин Олег Михайлович 190

ИНТЕГРИРОВАННЫЙ МОНИТОРИНГ ПОДВИЖНЫХ ОБЪЕКТОВ СВЯЗИ
Шостак Роман Константинович 192

ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИИ В СЕТЯХ С ВЫСОКИМ УРОВНЕМ КОНФИДЕНЦИАЛЬНОСТИ
Штаненко Василий Иванович, Барауля Игорь Геннадьевич, Маслов Олег Николаевич 193

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 195

ИССЛЕДОВАНИЕ СОЗДАНИЯ БЕЗОПАСНЫХ ПРОГРАММ ДЛЯ ВЫСОКОПРОИЗВОДИТЕЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ ПЛАТФОРМЫ
Бежан Роман Романович, Медведев Михаил Сергеевич, Арустамов Сергей Аркадьевич 195

УСЛОВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЛИНИЧЕСКОЙ СФЕРЕ СИСТЕМЫ ЗДРАВООХРАНЕНИЯ
Блюм Владислав Станиславович 196

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ НСД С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ОЦЕНКИ И АНАЛИЗА ЭМОЦИОНАЛЬНОЙ ЭКСПРЕССИИ И МИМИКИ ПОЛЬЗОВАТЕЛЯ
Брагина Елизавета Константиновна, Егоров Илья Эдуардович 205

СЕТЕВЫЕ АТАКИ СО СКРЫТИЕМ И СО ВСТАВКОЙ НА ПРИМЕРЕ SNORT, SURICATA И BRO
Браницкий Александр Александрович 209

АЛГОРИТМЫ ПАРАЛЛЕЛЬНОГО ПОИСКА ШАБЛОННЫХ ПОДСТРОК ПРИ РЕАЛИЗАЦИИ СИГНАТУРНЫХ ПРАВИЛ СОА
Браницкий Александр Александрович 210

КЛАССИФИКАЦИОННЫЕ ПРИЗНАКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ VANET
Буйневич Михаил Викторович, Столярова Екатерина Сергеевна, Хорошенко Сергей Викторович, Ширяев Денис Михайлович, Владыко Андрей Геннадьевич 212

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ КОНВЕРГЕНТНЫХ ТЕХНОЛОГИЙ В ОБЛАЧНОЙ СРЕДЕ
Воробьев Владимир Иванович, Левоневский Дмитрий Константинович, Рыжков Сергей Романович, Фаткиева Роза Равильевна 213

КВАЛИМЕТРИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ
Воробьев Владимир Иванович, Фаткиева Роза Равильевна 219

МЕТОДЫ ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ ЗАДАЧИ ПОИСКА УЯЗВИМОСТЕЙ В ИСПОЛНЯЕМЫХ ФАЙЛАХ
Демидов Роман Алексеевич 220

МОДЕЛИРОВАНИЕ И АНАЛИЗ ЗАЩИЩЕННОСТИ КОММУНИКАЦИОННОЙ СЕТИ УПРАВЛЕНИЯ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ НА БАЗЕ УСТРОЙСТВ XBEE
Десницкий Василий Алексеевич 221

МОДЕЛИ, МЕТОДИКА И АЛГОРИТМЫ ВЫБОРА ЗАЩИТНЫХ МЕР НА ОСНОВЕ СИСТЕМЫ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ ДЛЯ ПРОАКТИВНОГО И РЕАКТИВНОГО ПРОТИВОДЕЙСТВИЯ АТАКАМ В КОМПЬЮТЕРНЫХ СЕТЯХ
Дойникова Елена Владимировна, Котенко Игорь Витальевич 223

МОДЕЛЬ ЗАЩИЩЕННОГО ХРАНЕНИЯ БОЛЬШИХ СЛАБОСТРУКТУРИРОВАННЫХ ДАННЫХ
Евневич Елена Людвиговна, Петров Михаил Юрьевич 225

ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ «УМНЫЙ ГОРОД»
Жигадло Валентин Эдуардович 227

ОЦЕНКА ЭФФЕКТИВНОСТИ ПЛАТФОРМЫ РАСПРЕДЕЛЕННОГО АНАЛИЗА ДАННЫХ HADOOP В СРАВНЕНИИ С ПЛАТФОРМОЙ SPARK ДЛЯ ЦЕЛЕЙ СЕТЕВОЙ БЕЗОПАСНОСТИ
Кушнеревич Алексей Геннадьевич 228

АНАЛИЗ МЕТОДОВ ОБНАРУЖЕНИЯ МНОГОУРОВНЕВЫХ СТЕГАНОВСТАВОК В BMP-ИЗОБРАЖЕНИЯХ
Минаева Тамара Александровна, Волошина Наталия Викторовна, Беззатеев Сергей Валентинович 230

ПРИМЕНЕНИЕ ЯЗЫКА PYTHON ДЛЯ РАЗРАБОТКИ СРЕДСТВ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ
Никитин Андрей Сергеевич, Москвин Дмитрий Андреевич 235

ЭКОЛОГИЧЕСКИЙ КОНТРОЛЬ И РАЗВИТИЕ МОДЕЛЕЙ ПОПУЛЯЦИОННОГО РОСТА
Павлова Светлана Михайловна 236

МОДЕЛИРОВАНИЕ СЛОЖНЫХ МАШИНОСТРОИТЕЛЬНЫХ ИЗДЕЛИЙ В ХОДЕ ПРОИЗВОДСТВЕННЫХ ИСПЫТАНИЙ
Первухина Елена Львовна, Осипов Константин Николаевич, Голикова Виктория Викторовна 240

МЕТОДЫ ИЗВЛЕЧЕНИЯ ДАННЫХС ИЗОЛИРОВАННЫХ МАШИН
Романов Александр Алексеевич 244

БЛОКЧЕЙН-ТЕХНОЛОГИИ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ УПРАВЛЕНИИ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИМИ СИСТЕМАМИ
Токарев Алексей Игоревич 246

КОМПЛЕКСНАЯ СИСТЕМА ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ КАБИНЕТА РУКОВОДИТЕЛЯ. ЭФФЕКТИВНОСТЬ РАБОТЫ ПРИБОРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ КОМПЛЕКСНОЙ СИСТЕМЫ ИНЖЕНЕРНО ТЕХНИЧЕСКОЙ ЗАЩИТЫ КАБИНЕТА РУКОВОДИТЕЛЯ
Фаязов Кобилджон Абдукаюмович 247

ПРИМЕНЕНИЕ ДИНАМИЧЕСКОЙ МОДЕЛИ ПРОТИВОБОРСТВА ДЛЯ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННЫХ СИСТЕМ
Шишкин Владимир Михайлович, Колесников Константин Евгеньевич 251

МОДЕЛЬ ОБНАРУЖЕНИЯ ВНУТРЕННИХ НАРУШИТЕЛЕЙ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ БОЛЬШИХ ДАННЫХ
Ушаков Игорь Александрович, Котенко Игорь Витальевич 253

БАЗЫ ДАННЫХ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ: ПРИМЕНЕНИЕ SQL И NOSQL ТЕХНОЛОГИЙ
Ушаков Игорь Александрович, Котенко Игорь Витальевич 254

ВЛИЯНИЕ ДИНАМИКИ ИЗМЕНЕНИЯ ДАННЫХ НА ПРОЦЕСС КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ
Федорченко Андрей Владимирович, Котенко Игорь Витальевич 255

ФОРМАТЫ СОБЫТИЙ БЕЗОПАСНОСТИ В ПОДСИСТЕМЕ ЖУРНАЛИРОВАНИЯ ОС WINDOWS
Федорченко Андрей Владимирович, Чечулин Андрей Алексеевич, Дойникова Елена Владимировна 257

УГРОЗЫ БЕЗОПАСНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ И ЗАЩИТА ОТ ИНФОРМАЦИИ
Проноза Антон Александрович, Чечулин Андрей Алексеевич, Комашинский Николай Александрович 259

АВТОМАТИЧЕСКОЕ ВЫЯВЛЕНИЕ РАЗЛИЧИЙ В ИНТЕРЕСАХ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНОЙ СЕТИ В ЗАВИСИМОСТИ ОТ УКАЗАННЫХ ИМИ ПСИХИЧЕСКИХ ФУНКЦИЙ
Проноза Антон Александрович, Проноза Екатерина Валерьевна, Чечулин Андрей Алексеевич, Котенко Игорь Витальевич 261

СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ 264

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ VGATE R2
Бородин Михаил Константинович, Бородина Полина Юрьевна 264

ИДЕНТИФИКАЦИЯ ДВИЖУЩИХСЯ ОБЪЕКТОВ В ИНТЕЛЛЕКТУАЛЬНЫХ РАСПРЕДЕЛЕННЫХИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМАХ
Закасовская Елена Владимировна, Тарасов Валентин Сергеевич, Нютенко Сергей Игоревич 268

МОДЕЛИРОВАНИЕ СЛОЖНЫХ МАШИНОСТРОИТЕЛЬНЫХ ИЗДЕЛИЙ В ХОДЕ ПРОИЗВОДСТВЕННЫХ ИСПЫТАНИЙ
Первухина Елена Львовна, Осипов Константин Николаевич, Голикова Виктория 273

ОРГАНИЗАЦИЯ ДРЕВОВИДНЫХ ХРАНИЛИЩ ДАННЫХ С УЧЁТОМ РАЗМЕЩЕНИЯ В НИХ ЭЛЕКТРОННЫХ ПОДПИСЕЙ
Романова Юлия Николаевна, Янюшкин Константин Александрович 277

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 281

ВОЗМОЖНОСТИ СМИ В ТРАНСФОРМАЦИИ ПОЛИТИЧЕСКОГО СОЗНАНИЯ ОБЩЕСТВ СТРАН ЕАЭС
Гайшун Александр Николаевич 281

ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ В СЕТИ ИНТЕРНЕТ В ЕВРОПЕЙСКОМ СОЮЗЕ И РОССИЙСКОЙ ФЕДЕРАЦИИ
Долгошеин Пётр Сергеевич 283

ДУХОВНО-НРАВСТВЕННЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ИвентьевСергей Иванович 285

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ 289

ТЕОРИЯ ПРИНЯТИЯ РЕШЕНИЙ В ВОПРОСАХ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА
Большакова Людмила Валентиновна, Дашков Андрей Владимирович, Яковлева Наталья Александровна 289

О ПЕРСПЕКТИВАХ ПРИМЕНЕНИЯ ПРОСТРАНСТВЕННО-ВРЕМЕННОГО КОДИРОВАНИЯ В РАДИОЛИНИЯХ ВМФ
Типикин Алексей Алексеевич, Пуха Геннадий Пантелеевич 291

СТРАТЕГИИ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РЕГИОНАЛЬНЫХ ЭКОНОМИЧЕСКИХ СИСТЕМАХ С УЧЕТОМ РАЗНЫХ ТИПОВ РЕАКЦИЙ НА ВЫЗОВЫ ВНЕШНЕЙ СРЕДЫ
Титовец Алиса Юрьевна 292

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА ИТ-СПЕЦИАЛИСТОВ 296

РЕАЛИЗАЦИЯ КОМПЕТЕНТНОСТНОГО ПОДХОДА ПРИ ФОРМИРОВАНИИ ПООП НОВОГО ПОКОЛЕНИЯ НА ПРИМЕРЕ ЛАБОРАТОРНОГО ПРАКТИКУМА «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»
Барабаш Павел Александрович, Панасенко Михаил Александрович 296

ПРОФЕССИОНАЛЬНЫЙИ ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТЫ КАК ОСНОВА ВЗАИМОДЕЙСТВИЯ ОБРАЗОВАНИЯ, НАУКИ И ОТРАСЛЕВЫХРАБОТАДАТЕЛЕЙ В КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННОЙ ПОДГОТОВКЕ БУДУЩИХ КАДРОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕХНИЧЕСКОМ ВУЗЕ
Жигадло Анна Валентиновна, Одинокая Мария Александровна 299

ОСОБЕННОСТИ ПРОФЕССИОНАЛЬНОЙ И ОБРАЗОВАТЕЛЬНОЙ СТАНДАРТИЗАЦИИ В СФЕРЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СОВРЕМЕННОЙ ВЫСШЕЙ ШКОЛЕ
Жигадло Надежда Владимировна 300

ДИСТАНЦИОННОЕ ОБУЧЕНИЕ КАК ОПЕРАЦИОННО-ДИДАКТИЧЕСКАЯ ФОРМА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПЕДАГОГИЧЕСКИХ КАДРОВ В СИСТЕМЕ НЕПРЕРЫВНОГО ОБРАЗОВАНИЯ ВЗРОСЛЫХ
Каткова Ирина Васильевна, Цесаренко Ольга Петровна 301

КОНЦЕПЦИЯ СОЦИАЛЬНОЙ АДАПТАЦИИ СОТРУДНИКОВ СИЛОВЫХ МИНИСТЕРСТВ И ВЕДОМСТВ, УВОЛЕННЫХ В ЗАПАС
Михалев Юрий Валентинович, Хлюпин Владимир Алексеевич 305

МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ ЗАЩИЩЕННОСТИ ДАННЫХ ЭЛЕКТРОННОЙИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ УНИВЕРСИТЕТА
Соколов Сергей Сергеевич, Нырков Анатолий Павлович, Ковальногова Надежда Михайловна, Мамунц Давид Гарикович, Пастушок Елена Михайловна 309

ПЕДАГОГИЧЕСКИЕ И ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОГО ТЕСТИРОВАНИЯ НА РАЗНЫХ СТАДИЯХ ОБУЧЕНИЯ ДИСЦИПЛИНЕ
Титова Юлияна Францевна 312

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ 319

НАУЧНО-МЕТОДИЧЕСКИЕ ПОДХОДЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ТРАНСПОРТЕ
Белов Андрей Сергеевич, Барабанов Владимир Викторович 319

TOP-10 УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ VANET: АНАЛИТИЧЕСКИЙ ОБЗОР
Буйневич Михаил Викторович, Столярова Екатерина Сергеевна, Хорошенко Сергей Викторович, Ширяев Денис Михайлович, Владыко Андрей Геннадьевич 323

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДВИЖЕНИЯ СУДОВ
Бухарметов Максим Радикович, Нырков Анатолий Павлович 327

ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ РАБОТЫ ДОБЫВАЮЩИХ СКВАЖИН
Вирстюк Анастасия Юрьевна, Микшина Виктория Степановна, Ельмендеев Алик Питибаевич 329

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УПРАВЛЕНИИ ТРАНСПОРТОМ ГОРОДА, КАК ЭЛЕМЕНТ РЕАЛИЗАЦИИ КОНЦЕПЦИИ «УМНОГО ГОРОДА»
Жигадло Валентин Эдуардович 331

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОРСКИХ ТРАНСПОРТНЫХ СИСТЕМ
Константин Петрович Голоскоков, Марина Юрьевна Чиркова 332

ФЛЕШ-МОБ КАК ПРОТЕСТНАЯ ТЕХНОЛОГИЯ В ПОЛИТИЧЕСКОМ ДВИЖЕНИИ (НА ПРИМЕРЕ УКРАИНЫ)
Дегтярева Ольга Викторовна 334

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ИСПОЛЬЗОВАНИИ АВТОМОБИЛЬНОГО АВТОПИЛОТА
Кучеровская Олеся Владимировна 337

АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОВ ПРОНИКНОВЕНИЯ В КОМПЬЮТЕРНУЮ СИСТЕМУ
Лукин Евгений Игоревич, Прокопович Максим Сергеевич 339

АВТОМОБИЛЬНЫЙ КЛАСТЕР САНКТ-ПЕТЕРБУРГА
Поляков Дмитрий Сергеевич 342

ИСПОЛЬЗОВАНИЕ МЕТОДА ПОРТЕБИТЕЛЬСКОГО КОНТРОЛЯ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ
Селиверстов Ярослав Александрович, Селиверстов Святослав Александрович 343

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ 348

ПРОБЛЕМЫ СОЗДАНИЯ ИТ УПРАВЛЕНИЯ БОРЬБОЙ ЗА ЖИВУЧЕСТЬ ОМТ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ И ПЕРСПЕКТИВНЫЕ ПУТИ ИХ РЕШЕНИЯ
Алексеев Анатолий Владимирович, Соловьев Сергей Николаевич, Сус Герман Николаевич, Туркин Игорь Иванович, Москаленко Василий Александрович, Мусатенко Роман Иванович 348

РЕГРЕССИОННЫЙ АНАЛИЗ ДИНАМИКИ 10 ЛЕТ ХАКЕРСКИХ АТАК И ИНФОРМАЦИОННЫХ ИНЦИДЕНТОВ
Анциферов Александр Владимирович 350

АНАЛИЗ УЯЗВИМОСТЕЙ СЕРВИСОВАВТОРИЗАЦИИ И ВОЗМОЖНОСТИ ИХ СОВЕРШЕНСТВОВАНИЯ
Бирюкова Александра Валерьевна 352

УЯЗВИМОСТИ, УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОЦЕНКА СТЕПЕНИ ЗАЩИЩЕННОСТИ ДАННЫХ СЕРВИСА OUTLOOK
Кармазин Жан Романович 353

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В МОРСКОМ СЕКТОРЕ ЕВРОПЕЙСКОГО СОЮЗА
Колесникова Марина Львовна 354

ОСОБЕННОСТИ РАЗРАБОТКИ СИСТЕМ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ БОРЬБЫ ЗА ЖИВУЧЕСТЬ ПОДВОДНОЙ ЛОДКИ С УЧЕТОМ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Левоева Инга Валерьевна, Мудрова Алёна Александровна 358

УЯЗВИМОСТИ И ЗАЩИТА ANDROIDИIOSПРИЛОЖЕНИЙ
Повечеров Дмитрий Владимирович 360

ПРАКТИКА ТЕСТИРОВАНИЯ И ВОЗМОЖНОСТИ РАЗВИТИЯ ТЕХНОЛОГИЙ ПК «FORTINET»
Подгорнова Валерия Денисовна 361

ВИЗУАЛИЗИРОВАННЫЕ ЛОГИКО-ВЕРОЯТНОСТНЫЕ МОДЕЛИ СТРУКТУРНО-СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ
Поленин Владимир Иванович, Сущенков Дмитрий Андреевич 362

МЕТОДИКА ПОСТРОЕНИЯ ЛОГИКО-ВЕРОЯТНОСТНЫХ МОДЕЛЕЙ СТРУКТУРНО-СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ ДЛЯ ОЦЕНКИ РИСКА И БЕЗОПАСНОСТИ ИХ ФУНКЦИОНИРОВАНИЯ
Поленин Владимир Иванович, Потехин Александр Алексеевич 364

КОМПЬЮТЕРНЫЕ ВИРУСЫ: ИСТОРИЯ, КЛАССИФИКАЦИЯ, ПРОТИВОДЕЙСТВИЕ
Цыганков Илья Александрович 369

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОЛОГИИ 371

ЗАТМЕННОЕ ЗОНДИРОВАНИЕ ВЕРХНЕЙ АТМОСФЕРЫ ЗЕМЛИ С ПИЛОТИРУЕМОЙ ОРБИТАЛЬНОЙ СТАНЦИИ: ПОЛУЧЕНИЕ И СОХРАНЕНИЕ ИНФОРМАЦИИ
Бузников Анатолий Алексеевич 371

КОНЦЕПЦИЯ ВНУТРИЛАБОРАТОРНОГО КОНТРОЛЯ РЕЗУЛЬТАТОВ БИОТЕСТИРОВАНИЯ В ИСПЫТАТЕЛЬНЫХ ЭКОАНАЛИТИЧЕСКИХ ЛАБОРАТОРИЯХ ДЛЯ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОНТРОЛЯ ТОКСИЧНОСТИ ВОДНЫХ СРЕД
Величко Анна Николаевна 373

ЛОКАЛЬНЫЕ ФАКТОРЫ ГЛОБАЛЬНОГО ИЗМЕНЕНИЯ КЛИМАТА (К АНАЛИЗУ СИСТЕМ АТМОСФЕРНОГО МОНИТОРИНГА В МЕГАПОЛИСАХ)
Викторов Сергей Васильевич, Лабзовский Лев Дмитриевич 375

МАТЕМАТИЧЕСКИЕ МОДЕЛИ АНАЛИЗА ЭФФЕКТИВНОСТИ РАБОТЫ ДОБЫВАЮЩИХ СКВАЖИН
Вирстюк Анастасия Юрьевна, Микшина Виктория Степановна, Ельмендеев Алик Питибаевич 376

ДИСТАНЦИОННОЕ ЗОНДИРОВАНИЕ ПРИБРЕЖНЫХ ВОД ОХОТСКОГО МОРЯ: СРАВНЕНИЕ СПЕКТРОМЕТРИЧЕСКОГО И ЛИДАРНОГО МЕТОДОВ
Горяинов Виктор Сергеевич, Бузников Анатолий Алексеевич, Черноок Владимир Ильич..... 380

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ТОНКОПЛЕНОЧНЫХ СОЛНЕЧНЫХ МОДУЛЕЙ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ
Гульков Валерий Николаевич 381

МЕТОД ВОССТАНОВЛЕНИЯ ПРОФИЛЯ ВЕТРА ПО ОЦЕНКАМ ШИРИНЫ СПЕКТРА РАДИОЛОКАЦИОННОГО СИГНАЛА
Денисенков Дмитрий Анатольевич, Жуков Владимир Юрьевич, Щукин Георгий Георгиевич 382

ИНФОРМАЦИОННОЕ И ОПЕРАЦИОННОЕ ОБЕСПЕЧЕНИЕ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ДЕЯТЕЛЬНОСТИ СИЛОВЫХ СТРУКТУР И ОТРАСЛЕЙ ЭКОНОМИКИ РОССИИ
Доронин Александр Павлович, Щукин Георгий Георгиевич, Петроченко Вячеслав Михайлович, Козлова Наталья Александровна, Тимощук Александр Сергеевич, Шмалько Светлана Анатольевна. 384

ОСОБЕННОСТИ РЕШЕНИЯ ЗАДАЧ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ МЕГАПОЛИСА
Жигадло Валентин Эдуардович..... 387

ПРОБЛЕМЫ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О БЕЗОПАСНОСТИ ВОДНОЙ СРЕДЫ БИОТЕСТИРОВАНИЕМ НА ОСНОВЕ СУЩЕСТВУЮЩИХ НОРМАТИВОВ
Захаров Игорь Сергеевич..... 388

РАДИОЛОКАЦИОННЫЕ МЕТОДЫ ИЗМЕРЕНИЯ ГИДРОГРАФИЧЕСКИХ ПАРАМЕТРОВ МОРЯ
Орандаренко Елена Дмитриевна..... 389

ОЦЕНКА СТРУКТУРНОЙ ЗНАЧИМОСТИ ЭЛЕМЕНТОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА
Рябовая Валентина Олеговна..... 393

ГИБКИЕ ОРГАНИЧЕСКИЕ СОЛНЕЧНЫЕ ЭЛЕМЕНТЫ НА ОСНОВЕ СИСТЕМЫ «ФТАЛОЦИАНИН / ФУЛЛЕРЕН»
Тарасов Сергей Анатольевич 397

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ 399

ПРОБЛЕМА ЗАЩИТЫ ИНФОРМАЦИИ В МНОГОУРОВНЕВЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ
Бондаренко Игорь Борисович, Шиманчук Сергей Николаевич 399

АНАЛИЗ МЕТОДА БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ДЛЯ СИСТЕМЫ PAYPASS
Давыдов Вадим Валерьевич 402

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КИБЕРУСТОЙЧИВОСТЬ ЦИФРОВОЙ ЭКОНОМИКИ И ЦИФРОВОГО ПРОИЗВОДСТВА
Зегжда Петр Дмитриевич, Зегжда Дмитрий Петрович..... 406

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. ФИШИНГ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ЕМУ
Ильченко Лидия Михайловна, Уваров Роман Валерьевич, Зайцев Святослав Игоревич 407

ИСПОЛЬЗОВАНИЕ МОДЕЛЕЙ ВИЗУАЛИЗАЦИИ ДАННЫХ В DLP-СИСТЕМАХ
Коломеец Максим Вадимович..... 411

ПОИСК АНОМАЛИЙ В ПОВЕДЕНИИ ПРОГРАММНОГО ПРОЦЕССА С ПОМОЩЬЮ МАШИННОГО ОБУЧЕНИЯ
Лабутина Евгения Алексеевна..... 413

ПОДХОД К ПРОЕКТИРОВАНИЮ ЗАЩИЩЕННЫХ СИСТЕМ НА ОСНОВЕ ВСТРОЕННЫХ УСТРОЙСТВ
Левшун Дмитрий Сергеевич..... 414

ОРГАНИЗАЦИЯ КОЛЛЕКТИВНОГО УПРАВЛЕНИЯ БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ
Мариненков Егор Денисович, Шуваев Александр Константинович..... 416

ИССЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ СИСТЕМ УПРАВЛЕНИЯ МОБИЛЬНЫМИ УСТРОЙСТВАМИ
Медведев Михаил Сергеевич, Бежан Роман Романович, Арустамов Сергей Аркадьевич..... 418

ОЦЕНКА РИСКОВ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ И МЕТОДОЛОГИЙ
Мелешко Алексей Викторович, Чумак Евгений Александрович, Савков Сергей Витальевич 420

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ WSN-СЕТЕЙ НА ОСНОВЕ МОДЕЛИ ДОВЕРИЯ
Овасапян Тигран Джаникович, Иванов Денис Вадимович, Зегжда Дмитрий Петрович 421

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Орлов Иван Алексеевич 423

АНАЛИЗ ПОВЕДЕНЧЕСКИХ СВОЙСТВ СУБЪЕКТА ПРИ АУТЕНТИФИКАЦИИ НА ПРИМЕРЕ РУЧНОЙПОДПИСИ С ИСПОЛЬЗОВАНИЕМ АКСЕЛЕРОМЕТРА
Рудавин Николай Николаевич 425

МЕТОДИКИ И ИНСТРУМЕНТЫ АУДИТА СЕТЕВОЙ БЕЗОПАСНОСТИ
Садикова Анастасия Александровна, Титова Юлия Алексеевна, Савков Сергей Витальевич 430

ПОВЫШЕНИЕ ТОЧНОСТИ МЕТОДОВ СТЕГАНОАНАЛИЗА ПУТЕМ ОПТИМИЗАЦИИ ПАРАМЕТРОВ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ
Сивачев Алексей Вячеславович, Михайличенко Ольга Викторовна 435

ПРОБЛЕМА АНОНИМНОСТИ В СЕТИ ИНТЕРНЕТ.
СРАВНЕНИЕ МЕТОДОВ АНОНИМИЗАЦИИ ПОЛЬЗОВАТЕЛЯ
Титова Юлия Алексеевна, Садикова Анастасия Александровна, Савков Сергей Витальевич 437

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА: БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ 442

ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ В ГЛУБОКОМ АНАЛИЗЕ СЕТЕВОГО ТРАФИКА
Безверхняя Екатерина Александровна 442

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ
Бондарева Анастасия Дмитриевна, Гоман Елена Вячеславовна 443

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАЩИЩЕННОСТИ ОСУЩЕСТВЛЕНИЯ ФИНАНСОВЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЕСКОНТАКТНОЙ ОПЛАТЫ
Ганчикова Юлия Сергеевна, Курышева Алена Андреевна 445

ОБЗОР DLPСИСТЕМ
Герцен Дмитрий Михайлович, Стафеев Алексей Владимирович, Сердюков Никита Васильевич .. 446

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ОДНОРАЗОВОГО БЛОКНОТА
ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ ПОТОКОВ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА
Грозов Владимир Андреевич 451

ОСНОВНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СКЛАДА,
РАБОТАЮЩЕГО ПОД УПРАВЛЕНИЕМ WMS-СИСТЕМЫ
Губа Евгений Александрович 452

МОДЕЛИРОВАНИЕ ОРГАНИЗМА ЧЕЛОВЕКА ДЛЯ ПОДДЕРЖКИ ВРАЧЕБНЫХ РЕШЕНИЙ
Губин Александр Вадимович, Игнатьев Михаил Борисович, Катермина Татьяна Сергеевна, Красников Андрей Георгиевич 454

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ BIGCODEДЛЯ ОЦЕНКИ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
Заколдаев Данил Анатольевич, Римша Андрей Сергеевич, Югансон Андрей Николаевич 455

ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ НАЗЕМНОГО ГОРОДСКОГО ПАССАЖИРСКОГО ТРАНСПОРТА
Ильченко Лидия Михайловна, Зайцев Святослав Игоревич 458

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК СПОСОБ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СВЕДЕНИЯМ, СОСТАВЛЯЮЩИМ КОММЕРЧЕСКУЮ ТАЙНУ
Кизрякова Анастасия, Солодовников Владислав 462

МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ КАК СПОСОБ ПОЛУЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА
Кизрякова Анастасия, Солодовников Владислав 465

ПРИМЕНЕНИЕ НОВЫХ МОДЕЛЕЙ ВИЗУАЛИЗАЦИИ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРИНИМАЕМЫХ ПОЛЬЗОВАТЕЛЕМ СИСТЕМЫ РЕШЕНИЙ
Коломеец Максим Вадимович, Чечулин Андрей Алексеевич 466

ИДЕНТИФИКАЦИЯАТАКНАБЕСПРОВОДНУЮ СЕНСОРНУЮ СЕТЬ НА ОСНОВЕ АНАЛИЗА ПОВЕДЕНИЯ СЕТИ
Коржук Виктория Михайловна ... 468

АНАЛИЗ ЗАЩИЩЕННОСТИ ERP-СИСТЕМ. ОБЩИЙ ПОДХОД К АНАЛИЗУ
Кривдюк Надежда Михайловна ... 469

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАЩИЩЕННОСТИ ОСУЩЕСТВЛЕНИЯ ФИНАНСОВЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ
Курышева Алена Андреевна, Ганчикова Юлия Сергеевна ... 470

МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ КЕСМ-СИСТЕМАМ
Лейфер Анастасия Александровна ... 471

СИСТЕМА СБОРА И АНАЛИЗА ДАННЫХ ДЛЯ ИССЛЕДОВАНИЯ УНИКАЛЬНОСТИ ПОВЕДЕНЧЕСКИХ ПРИЗНАКОВ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ УСТРОЙСТВ
Лейфер Кирилл Ильич ... 474

АНАЛИЗ СУЩЕСТВУЮЩИХ ДАТЧИКОВ ДЛЯ ВЫЯВЛЕНИЯ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ
Лисецкая Кристина Валерьевна ... 476

АНАЛИЗ ВОПРОСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ МЕДИЦИНСКОГО НАЗНАЧЕНИЯ
Лосев Роман Вячеславович, Ручкан Александр Дмитриевич ... 476

ОБЗОР СУЩЕСТВУЮЩИХ РЕШЕНИЙ СИСТЕМ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Лямзина Алиса Григорьевна, Коржук Виктория Михайловна ... 477

ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ МЕТОДА КУСТА СОБЫТИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Наумов Андрей Дмитриевич, Попов Илья Юрьевич ... 478

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ПРИМЕРЕ ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ
Сазонов Антон Борисович, Немченко Алексей Алексеевич ... 480

РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД К ПРОВЕДЕНИЮ И ОБЕСПЕЧЕНИЮ ВНУТРЕННЕГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Созинова Екатерина Николаевна ... 481

МЕТОД ПРОВЕДЕНИЯ ВНУТРЕННЕГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ
Созинова Екатерина Николаевна ... 483

ПРОБЛЕМА НЕСООТВЕТСТВИЯ СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ СОВРЕМЕННЫМ ТРЕБОВАНИЯМ МЕР ФИЗИЧЕСКОЙ ЗАЩИТЫ
Федорова Алёна Владимировна, Алексеев Дмитрий Станиславович ... 484

МЕТОДИКА ПРЕДВАРИТЕЛЬНОЙ ОБРАБОТКИ ГРАФИЧЕСКИХ ОБЪЕКТОВ ДЛЯ ЗАДАЧИ ИДЕНТИФИКАЦИИ В ВИДЕОПОТОКЕ
Шевченко Денис Алексеевич ... 485

ОБНАРУЖЕНИЕ МЕСТ НАРУШЕНИЯ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ РЕСУРСОВ В ПРОГРАММНОМ КОДЕ
Цветков Лаврентий Викторович, Спивак Антон Игоревич ... 488

МОДЕЛЬ ОБНАРУЖЕНИЯ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ НА МУЛЬТИАГЕНТНЫЕ РОБОТОТЕХНИЧЕСКИЕ СИСТЕМЫ
Юрьева Радда Алексеевна, Тимко Андрей Сергеевич, Комаров Игорь Иванович ... 491

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОБЛЕМЫ УСТОЙЧИВОГО РАЗВИТИЯ ... 493

ДЕЛОВАЯ ИГРА «МОДЕЛИРОВАНИЕ ГОРОДА КАК СЛОЖНОЙ САМООРГАНИЗУЮЩЕЙСЯ ЧЕЛОВЕКО-МАШИННОЙ СИСТЕМЫ»
Игнатьев Михаил Борисович ... 493

К ВОПРОСУ О СОЗДАНИИ НОВОГО ЗДАНИЯ МУЗЕЯ ОБОРОНЫ И БЛОКАДЫ ЛЕНИНГРАДА
Игнатьев Михаил Борисович, Макин Алексей Иванович, Мамошин Михаил Александрович, Никитин Александр Иванович, Фадеева Нина Владимировна ... 494

ОБ УПРАВЛЕНИИ РОБОТОТЕХНИЧЕСКИМИ СИСТЕМАМИ В ТРЕХМЕРНОМ ПРОСТРАНСТВЕ
Игнатьев Михаил Борисович, Катермина Татьяна Сергеевна, Липинский Ян Александрович, Ненашев Вадим Александрович 495

ИНТЕНЦИОНАЛЬНЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ НА ОСНОВЕ ЛИНГВО-КОМБИНАТОРНОГО МОДЕЛИРОВАНИЯ
Игнатьев Михаил Борисович 496

МОДЕЛЬНОЕ ПРЕДСТАВЛЕНИЕ ИЗДЕЛИЙ ПРОГРАММИРУЕМОЙ ЛОГИКИ В ЗАДАЧАХ ОБРАТНОГО ПРОЕКТИРОВАНИЯ
Быков Андрей Владимирович, Демченко Олег Анатольевич, Усатый Вадим Анатольевич 497

СТРЕЛА ВРЕМЕНИ И НЕОБРАТИМОСТЬ ПРОЦЕССОВ В СЛОЖНЫХ ДИНАМИЧЕСКИХ СИСТЕМАХ
Острейковский Владислав Алексеевич, Муравьев Игорь Измайлович, Шевченко Елена Николаевна 500

ПОДХОДЫ К ОЦЕНКЕ НАДЕЖНОСТИ СЛОЖНЫХ СИСТЕМ
Свеженцев Игорь Иванович 505

ОГЛАВЛЕНИЕ 508

CONTENTS

STATE POLICY IN THE SPHERE OF INFORMATIZATION AND INFORMATION SECURITY……5

INFORMATIZATION OF THE TAX SPHERE IN THE MODEL OF THE IDEAL CITY
Eremichev Daniil..... 5

PROBLEMS OF CREATION OF THE SITUATIONAL CENTERS OF TERRITORIAL SUBJECTS OF THE FEDERATION IN THE CONDITIONS OF TRANSITION TO DIGITAL ECONOMY
Zhigadlo Valentin..... 7

THE PROBLEMS OF SMART CITY
Zykova Galina, Artamonov Leonid, Elezov Valentine..... 13

METHODOLOGICAL AND METHODICAL BASES OF CREATION AND APPLICATION OF DISASTER TOLERANT INFORMATION SYSTEMS
Okhtilev Mikhail, Klucharev Alecsandr, Sokolov Boris, Yusupov Rafael'..... 15

NOOSPHERE EDUCATION IN THE DEVELOPED INFORMATION SOCIETY
Sovetov Boris..... 17

APPLICATION OF SPACE ACTIVITY RESULTS IN THE INTERESTS OF PROVIDING INFORMATION AND ECONOMIC SECURITY IN RUSSIAN FEDERATION REGIONS
Usaty Vadim, Iushchenko Sergei..... 20

DIAGNOSTICS OF INFRINGEMENTSOF INFORMATION SECURITY BASED ON ARTIFICIAL NEURAL NETWORKS IN INFORMATION AND COMMUNICATION SYSTEMS
Avramenko Vladimir, Malikov Albert..... 24

INFORMATION SECURITY OF TELECOMMUNICATION NETWORKS..... 26

PREDICTING THE PROTECTION OF INFORMATION IN AUTOMATED SYSTEMS
Avramenko Vladimir, Bedenkov Viktor, Selyakov Maxim..... 26

ASSESSMENT OF NETWORK COMPUTER SECURITY RISKS ON BASIS OF THE FUZZY LOGICAL INFERENCE
Ageev Sergey, Saenko Igor..... 28

MEANS AND METHODS OF PROTECTION OF INFORMATION RESOURCES
Alasheev Vadim, Latushko Nikolay..... 30

DEPLOYMENT OF VIRTUAL INFRASTRUCTURE REMOTE TRAINING IN THE EXISTING AUTOMATED CONTROL SYSTEM
Alekseev Oleg, Nogin Sergei, Chesnokov Alexander..... 32

IMPLEMENTATION OF «INFRASTRUCTURE AS SERVICE» SERVICE FOR CONDUCTING INTEGRATED PRACTICAL LESSONS WITH OFFICERS OF THE GOVERNING BODY
Alekseev Oleg, Nogin Sergei, Chesnokov Alexander..... 33

INDEXES OF SECURITY OF INFORMATION EXCHANGE IN AUTOMATED CONTROL SYSTEMS OF COMMUNICATION OF SPECIAL PURPOSE
Bashkirtsev Andrey..... 35

ORGANIZATION OF ACCES TO RESOURCES OF NETEROGENEOUS MEDIA AUTOMATION
Bashkirtcev Andrey, Zibrov Oleg, Zobnin Konstantin, Usachev Igor..... 36

FIREWALLS AN ELEMENT OFCONTROL SYSTEMS INFORMATION SECURITY ARCHITECTURE OF CONTEMPORARY TELECOMMUNICATION NETWORKS AND DATA CENTERS
Bashkirtsev Andrey, Mikhailichenko Nikolay, Parashchuk Igor..... 38

PROBLEMS OF MODELING MODERN COMMUNICATION SYSTEMS
Bezzubov Oleg..... 39

SECURITY OFSTATE INFORMATION SYSTEMS
Bezugly Yuri, Vershennik Alex, Vershennik Elena, Starodubtsev Yuri..... 42

PROTECTION OF SELF-ORGANIZINGNETWORKS IN THE RANGE OF POVER STRUCTURES
Beskov Andrey, Votinov Mikhail, Kovaykin Yuri, Krivoshey Yulia..... 43

ORGANIZATIONAL-TECHNICALCOOPERATION POLISARIOCONTROLLED AT COMPUTER INTELLIGENCE
Beskov Andrey, Kiryanov Alexander, Kovaykin Yuri, Najafov Haji, Uimanov Andrey..... 45

THEFEATURESOFDISCRETIONARY ACCESS CONTROLMODEL IMPLEMENTATION BY ROLE BASED ACCESS CONTROL MODEL FACILITIES
Biryukov Mikhail, Volkova Evgeniya, Saenko Igor 47

THE METHOD OF MANDATORY ACCESS CONTROL IMPLEMENTATION BY ROLE BASED ACCESS CONTROL FACILITIES
Biryukov Mikhail, Zibrov Oleg, Saenko Igor 49

ORGANIZATION OF PROTECTING PROCESSES IN THE INFORMATION- TELECOMMUNICATION SYSTEM
Borets Dmitry, Kovalev Igor, Malyshev Viktor, Pantyukhin Oleg 50

EVALUATION OF THE OPERABILITY
OF THE LOCAL AREA NETWORK OF THE CONTROL CENTER OF THE POWER DEPARTMENT
Borets Dmitry, Kovalev Igor, Malyshev Viktor, Pantyukhin Oleg 52

TECHNICAL ORDNANCE OF INFORMATION SYSTEMS
Borisov Aleksey, Vladimirov Dmitrii 54

ANALYSIS OF PROBLEMS OF DEVELOPMENT OF ASU OF A SPECIAL PURPOSE
Borisov Alexander, Loginov Vyacheslav, Pimenov Aleksey 55

THE TIME SIGNS OF NETWORK AND NETWORK PARTS SECURITY IN CYBER ATTACKS
Brechko Alexandr, Lvova Nataliya, Latushko Nikolay 56

OVERVIEW OF ENCRYPTION METHODS
Bukhanov Pavel, Smirnov Dmitry, Khan Georgiy, Birukov Mikhail 58

FUNCTIONAL-DISCRETIONARY MODEL OF ACCESS CONTROL
Valyushkina Julia 60

APPROACH TO COUNTERING COMPUTER ATTACKS ON CRITICAL INFORMATION SEGMENTS OF A SPECIAL PURPOSE NETWORK
Vasyukov Dmitry, Smygin Alexander, Mitrofanov Mikhail 61

SECURITYISTHEPROBLEMOFTHEUSERINTERFACE
Vertepov Mikhail, Bukreev Denis, Gavrilenko Vladimir 63

METHOD OF PROTECTING SUBSCRIBER LINES
Vershennik Alex, Vershennik Elena, Kupriyanov Nikita, Starodubtsev Yuri 64

CONCEPTUAL APPROACHES TO THE PROBLEM OF ENSURING INFORMATION SECURITY OF COMPLEXES WITH UNMANNED AERIAL VEHICLES
Vinokurov Aleksandr, Lozovskiy Vladimir, Kibenko Aleksandr 66

PROTECTION OF MICROPROCESSOR MEANS OF DATA PROCESSING FROM INTENTIONAL POWER ELECTROMAGNETIC INFLUENCES
Vladimirov Dmitrii, Borisov Aleksey 68

ABOUT THE COMMUNICATION NETWORK MODELLING FACILITIES
Volkova Evgenia, Chukarikov Aleksandr 69

PROTECTION OF INFORMATION IN THE SYSTEMS OF TRANSMISSION, STORAGE AND PROCESSING OF INFORMATION
Volostnykh Viktor, Rogov Ruslan, Mitrofanov Mikhail 71

SOME METHODS OF NETWORK ANALYSIS
Gapochkin Artem, Mikhaylichenko Nikolay 72

THE USE OF NEURAL NETWORKS TO DETECT NETWORKS ATTACKS
Gladkov Vladimir, Taraskina Anastasiya, Kyznecov Sergey, Tesla Sergey, Akishin Andrey 73

THE EVENTS PLANNING OF THE OPERATIONAL-TECHNICAL SERVICES FOR FACILITIES AUTOMATION SPECIAL PURPOSE
Grigoryan Vazgen, Kulikov Vladimir, Pantyukhin Oleg, Solodukhin Boris 75

THE PROTECTION OF INFORMATION FROM UNAUTHORIZED ACCESS IN AUTOMATED SYSTEMS UNDER THE MANAGEMENT OF THE SPECIAL EDITION OPERATIONAL SYSTEM ASTRA LINUX SE
Grin Daria, Ilina Olga, Kupchinenko Olga, Skoropad Aleksandr 76

TO THE QUESTION OF IMPROVING THE EFFICIENCY OF THE EVERYDAY ACTIVITY OF THE GOVERNING BODY
Guryev Sergei, Scherbakov Aleksandr 78

ABSOLUTELY STANDBY QUANTUM ENCRYPTION
Gushchin Igor, Petrenko Mikhail, Ovchinnikov Nikolay 79

SOME FEATURES OF THE FUNCTIONING OF INFORMATION SECURITY SYSTEM UNDER INTERACTION OF REGIONAL CORPORATE TELECOMMUNICATION NETWORKS WITH A COMMON USE NETWORK
Dediourin Anton, Yerichev Pavel, Parashchuk Igor 81

TYPES OF MEANS OF TRUSTED DOWNLOADS FACILITIES AND THEIR ROLE IN SECURING THE INFORMATION SECURITY OF TELECOMMUNICATION NETWORKS
Zhmurov Vladislav, Parashchuk Igor, Sayarkin Leonid 83

THE WAY OF PROTECTION OF RESOURCES OF A MULTISERVICE COMMUNICATION NETWORK
Zhuravel Evgeny 85

SAFETY OF MANAGEMENT OF ROBOTIC SYSTEMS ON THE BASIS OF ARTIFICIAL INTELLIGENCE WITH APPLICATION OF NEURAL NETWORKS
Zakharov Ruslan, Lauta Oleg, Kribel Aleksandr, Soloviov Dmitriy 92

ANALYSIS OF APPLICATION TRENDS AND ISSUES OF SECURITY OF INFORMATION SYSTEMS OF DATA STORAGE FOR CLOUD TECHNOLOGIES
Ziyaev Pavel, Parashchuk Igor, Tkachenko Vladimir 93

METHOD OF MEASUREMENT OF IONOSPHERE PARAMETERS FOR ESTIMATION OF PROPERTIES AND CHARACTERISTICS OF SATELLITE RADIOCOMMUNICATION
Zorin Vladimir, Koryakin Denis, Andreev Gleb 95

THE VPN TECHNOLOGY APPLICATION ASPECTS IN CRITICAL INFRASTRUCTURE
Zubakin Vladimir, Kiy Andrey, Morozov Ivan 97

STATEMENT OF THE PROBLEM POSITIONING CONTROLLER ON SOFTWARE DEFINED NETWORKING
Zubakin Vladimir, Hmellyar Nikolai, Shinkarev Semyon 99

MODEL OF THE INFRINGER IN PROVIDING INFORMATION SECURITY BASED ON ABDUCTIVE SYNTHESIS OF STRUCTURES OF SCENARIOS
Karganov Vitaly, Lipatnikov Valery 100

MODEL OF THREATS TO INFORMATION SECURITI AT THE OBJEKT OF INFORMATIZAZION
Karpov Aleksander 102

APPROACHES TO IMPROVING THE SYSTEM FOR MONITORING THE STATE OF INFORMATION SECURITI AT THE CONTROL SITE
Karpov Aleksander, Lepeshkin Oleg 104

TECHNIQUE OF FORECASTING OF LEGAL IMPACTS ON ROBOTIC SYSTEMS
Kocinyak Mikhail, Dementiev Vladislav, Teslya Sergei, Lauta Oleg 106

INFORMATION SECURITY NETWORKS IEEE 802.11
Kolnoochenko Anastasiya 107

CRYPTOGRAPHIC PROTECTION OF A CONTROL PATH OF ROBOTIC SYSTEMS
Kocinyak Mikhail, Gudkov Mikhail, Safonov Alexey, Arutunyan Boris 108

METHOD OF PREDICTING THE IMPACT OF A TARGETED CYBERNETIC ATTACK ON THE INFORMATION AND TELECOMMUNICATIONS NETWORK
Kociniak Mihail, Ivanov Denis, Lauta Oleg, Nechepurenko Aleksandr, Murtazin Ildar 109

APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS IN TASKS OF INFORMATION SECURITY SUPPORT
Kireev Sergey 111

THE PROBLEM OF ORGANIZATION TECHNICAL COUPLING SYSTEM OF PROTECTION OF INFORMATION OF VARIOUS AUTOMATED CONTROL SYSTEM OF SPECIAL PURPOSE
Kondrashov Yuri, Maksimenko Yevgeniy 113

SSESSMENT METHODOLOGY OF INTEGRATED INFORMATION IMPACT OF INFORMATION AND TELECOMMUNICATION SYSTEMS SPECIAL PURPOSE
Kocinac Michael, Yastrebov Vladimir, Klinshov Ilya, Gulevich Anton 114

INFORMATION SECURITY, TRANSFERRED ON INFORMATION AND TELECOMMUNICATION CHANNELS OF MAIL SERVERS
Kribel Alexander, Denis Koryakin 115

PROBABILISTIC AND TIME CHARACTERISTICS OF THE ATTACKS TO ROBOTIC SYSTEMS
Kuznetsov Sergey, Ivanov Denis, Vlasenko Maxim, Latushko Nikolay 117

THE STABILITY OF THE INFORMATION AND TELECOMMUNICATIONS NETWORK IN THE CONDITIONS OF COMPUTER ATTAKS
Kuznesov Sergey, Novikov Pavel, Kuznesova Anastasya 118

A METHOD FOR REDUCING THE OVERHEAD IN A PACKET DATA NETWORK
Kurashev Zaur 119

THE APPROACH TO THE SECURITY ASSESSMENT OF INFORMATION-TELECOMMUNICATION NETWORKS OF SPECIAL PURPOSE FROM TECHNICAL COMPUTER INTELLIGENCE
Lauta Oleg, Klinshov Ilya, Yastrebov Vladimir, Rusakov Yegor 121

PROBLEMSANDWAYS OF SECURITY SATELLITE COMMUNICATIONS
Lebeda Evgeny, Tarasov Aleksandr 123

DEVELOPMENT OF THE SCIENTIFIC AND METHODOLOGICAL APPARATUS FOR IDENTIFICATION AND FORECASTING THE EVOLUTION OF INTER-ETHNIC AND INTER-CONFLICTIONAL CONFLICTS ARISING FROM THE RESULT OF INFORMATION INFECTIONS
Lozovskiy Vladimir, Vinokurov Aleksandr, Galickiy Valeriy 125

MODELING WAYS ANALYSIS OF CONFLICT SITUATIONS IN CYBERSPACE
Lvova Nataliya, Brechko Alexandr, Balenko Olga 127

THE USE OF PROGRAMMABLE LOGIC CONTROLLERS FOR VOLTAGE MEASUREMENT IN POWER SUPPLY NETWORKS
Mel' Mikhail, Shukin Andrey 129

QUESTIONS OF PROTECTING THE INTERESTS OF THE RUSSIAN FEDERATION IN THE INFORMATION SPACE
Neizhmak Alexey 130

PROTECTION OF INFORMATION FROM UNAUTORIZED ACCESS
Mekhryakov Alexandr, Shibanov Danil, Trifonov Pavel, Birukov Mikhail 132

SECURITY OF TELECOMMUNICATION NETWORKS BASED ON THE SELECTION OF PROTECTED INTERVALS WHEN JAMMING
Mitrofanov Michael, Rakitskiy Stanislav, Chikov Dmitry 134

RESEARCH OF DESIGNING PROGRAM-CONFIGURABLE NETWORKS
Mikhailov Vyacheslav, Il'ichev Svyatoslav, Fedoseev Denis, Stepanova Elena 135

PROBLEMS AND PROSPECTS OF DATA CENTERS SECURITY
Mikhaylichenko Nikolay 137

PROBLEMS OF INFORMATION SECURITY IN MOBILE DEVICES AND POSSIBLE WAYS OF THEIR SOLUTIONS
Neizhmak Alexey 139

INVESTIGATION OF THE PROBLEM OF LISTENING THE NETWORK TRAFFIC
Nehan' Evgeny, Gudkov Mikhail 141

TO THE QUESTION OF FUNCTIONAL, ORGANIZATIONAL AND STRUCTURAL CONSTRUCTION OF THE INFORMATION SECURITY SYSTEM UNDER INTERACTION OF REGIONAL CORPORATE TELECOMMUNICATION NETWORKS WITH A COMMON USE NETWORK
Nyagan Evgeny, Parashchuk Igor, Skryabin Evgeny 142

MODELS OF INTELLECTUAL INFLUENCES
Nechepurenko Aleksandr, Suetin Artem, Murtazin Ildar, Lauta Oleg 144

MODELING OF BROADBAND RADIO ACCESS NETWORKS BASE STATIONS ALLOCATION
Ovsyannikov Stanislav, Panin Roman, Kalyuka Vladimir 146

INFORMATION SECURITY PRINCIPLES OF WIRELESS SUBSCRIBER ACCESS NETWORKS
Ovsyannikov Stanislav, Panin Roman, Kalyuka Vladimir 147

NEURAL NETWORK APPLYING FOR SIGNAL'S DEMODULATION
Petrenko Mikhail, Ovchinnikov Nikolay 149

INFORMATION SECURITY OF THE TELECOMMUNICATION COMPONENT CYBERPHYSICAL SYSTEMS
Parashchuk Igor 150

PROBLEMS OF PLANNING THE APPLICATION OF DEPO SPECIAL PROCESSING CENTERS
Pimenov Aleksey, Denzhonkov Kirill,Borisov Alexander, Prudnikov Evgeny 152

THEMODELING METHODS OF COMMUNICATION NETWORKS WITH PACKET RADIO NETWORKS
Popov Andrey, Mikhaylichenko Nikolay 154

METHOD OF RANDOMIZED CONSOLIDATED INDICATORS FOR EXPERT EVALUATION OF INFORMATION PROTECTION SYSTEMS
Popova Elena 155

ELECTRONICS OF THE INTERFERENCE CODIFICATION FOR DATA TRANSMISSION CHANNELS
Prudnikov Evgeny, Pimenov Aleksey, Asheulov Sergey 158

ASSESSMENT ANALYSIS OF THE PROBLEM OF INFORMATION RESOURCES ACCESS CONTROL IN CLOUDY INFRASTRUCTURES
Saenko Igor 159

DEVELOPMENT OF A METHOD TO SUPPORT DECISION-MAKING ON THE CHOICE OF HARDWARE AND SOFTWARE MODULES TRUSTED BOOT TO PROTECT AGAINST UNAUTHORIZED ACCESS TO WORKSTATION OF OFFICIALS OF LAW ENFORCEMENT AGENCIES IN TELECOMMUNICATION NETWORKS
Sayarkin Leonid 161

UNITED ARCHITECTURE OF SECURITY FOR PROTECTION OF THE CORPORATE NETWORK
Selyakov Maxim, Pashchenko Vasily, Bedenkov Victor, Matveyev Alexander 162

METHODSOFINFORMATIONPROTECTION IN APPLICATIONS ON THE ASP.NET PLATFORM
Skryabin Evgeny, Zajcev Danila 164

ABOUT THE PROBLEM OF CONTROL OF THE VIRTUAL LOCAL COMPUTER NETWORKS IN CORPORATE INFORMATION SYSTEMS
Starkov Artyom, Saenko Igor 166

ASSIGNMENT ANALYSIS OF KEY TASKS IN THE MANAGEMENT OF THE COMMUNICATION NODE A SPECIAL PURPOSE
Sutyrin Vyacheslav, Khmelevskoy Valerij 168

REQUIREMENTS VOZMOJNOSTYAM FUNCTION "ACCOUNTING", IMPLEMENTED WITH AUTOMATION MANAGEMENT NODE A SPECIAL PURPOSE
Sutyrin Vyacheslav, Khmelevskoy Valerij 169

AN APPROACH TO CREATION OF THE SIMULATION MODEL FOR THE ROBOTIC COMPLEX INFORMATION SECURITY SYSTEM
Teplov Ivan, Mahnach Andrey, Saenko Igor 171

APPROACH TO THE RATIONALE OF REQUIREMENTS TO THE PROTECTION RESOURCES OF THE INFORMATION AND TELECOMMUNICATION NETWORK
Teslia Sergey, Martynyuk Ivan, Fedorova Svetlana, Chop Aleksey 172

ENSURING INFORMATION SECURITY OF DATA STORAGE NETWORKS
Tkachenko Vladimir 174

SAFETY IN MOBILE COMMUNICATION NETWORKS
PROTECTION OF INFORMATION RESOURCES IN NETWORKS 4G
Ulyanov Maxim, Godunov Evgenij, Terekhov Alexander 175

TO THE QUESTION ABOUT THE PROBLEM OF INFORMATION SECURITY IN AUTOMATED SYSTEMS SPECIAL PURPOSE
Usachev Igor, Kiy Andrey, Zibrov Oleg, Bashkirtsev Andrey, Sherbakov Alexandr 177

NETWORK MONITORING SOFTWARE TO PROVIDE INFORMATION SECURITY
Fedoseev Denis, Koryakin Denis, Yastrebov Egor 179

THE DESIGN METHOD OF SYSTEM ACCESS SECURITYAUTOMATED INFORMATION SYSTEMS
Fialkin Ilya 181

ANALYSIS OF POSSIBILITIES USING A HASH FUNCTION FOR TEXT COMPARISON WITHOUT OPENING THE CONTENTS
Khilko Valeriy, Levkin Aleksandr 183

SEARCH FOR COPIES IN SOURCE CODE
Khilko Valery, Sharov Ilya 184

A MODEL FOR DETERMINATION OF SECRECY COMMUNICATION SYSTEM
Hudaynazarov Yuri, Maslov Oleg, Baraulya Igor 185

THE NEED FOR THE DEVELOPMENT OF THE SYSTEM REQUIREMENTS OPERATING SYSTEMS OF SPECIAL PURPOSE
Chesnokov Alexander, Yudin Anatoly, Alekseev Oleg 187

PROGRAM FOR MODELING OBJECTS – SKETCHUP
Shibanov Danil 189

THE RELEVANCE OF THE DEVELOPMENT OF NETWORK MONITORING SECURITY INFORMATION SYSTEMS
Shostak Roman, Lepeshkin Oleg 190

THE APPROACH OF INTEGRATED MONITORING OF MOBILE OBJECTS OF COMMUNICATION
Shostak Roman 192

THE DESIGN METHOD OF SYSTEM ACCESS SECURITY
Shtanenko Vasily, Baraulya Igor, Maslov Oleg 193

SAFETY OF INFORMATION TECHNOLOGIES 195

RESEARCH OF CREATION OF SAFE PROGRAMS FOR THE HIGH-PERFORMANCE COMPUTING PLATFORM
Bezhan Roman, Medvedev Mikhail, Sergey Arustamov 195

CONDITIONS OF INFORMATION SECURITY IN THE CLINICAL SPHERE OF THE HEALTH SYSTEM
Blum Vladislav 196

INCREASING THE PROTECTION OF INFORMATION FROM UNAUTHORIZED ACCESS USING BIOMETRIC AUTHENTICATION
Bragina Elizaveta, Egorov Ilia 205

EVASION AND INSERTION NETWORK ATTACKS ON THE EXAMPLE OF SNORT, SURICATA AND BRO
Alexander Branitskiy 209

CLASSIFICATION FEATURES OF INFORMATION SECURITY THREATS IN VANET
Mikhail Buinevich, Ekaterina Stolyarova, Sergei Khoroshenko, Denis Shiryaev, Andrei Vladyko 212

SECURITY MANAGEMENT OF CONVERGENT TECHNOLOGIES IN THE CLOUDY ENVIRONMENT
Vorobiev Vladimir, Levonevskii Dmitrii, Ryzhkov Sergei, Fatkieva Roza 214

QUALIMETRY OF INFORMATION ASSET SECURITY
Vorobiev Vladimir, Fatkieva Roza 219

DEEP LEARNING METHODS FOR VULNERABILITY SEARCH IN EXECUTABLE CODE
Demidov Roman 220

MODELING AND SECURITY ANALYSIS OF A COMMUNICATION NETWORK FOR CRISIS MANAGAMENT ON THE BASE OF XBEE DEVICES
Desnitsky Vasily 221

MODELS, TECHNIQUE AND ALGORITHMS OF THE COUNTERMEASURE SELECTION BASED ON THE SYSTEM OF SECURITY METRICS FOR THE PROACTIVE AND REACTIVE RESPONSE TO ATTACKS IN COMPUTER NETWORKS
Doynikova Elena, Kotenko Igor 223

SEMI-STRUCTURED BIG DATA PROTECTED STORAGE MODEL
Evnevich Elena, Petrov Mikhail 225

PRINCIPLES OF CREATION OF THE «SMARTCITY» SYSTEM
Zhigadlo Valentin 227

EVALUATION OF THE EFFICIENCY OF HADOOP DISTRIBUTED DATA ANALYSIS PLATFORM IN COMPARISON WITH SPARK PLATFORM FOR NETWORK SECURITY GOALS
Kushnerevich Alexey 228

ANALYSIS OF STEGANOANALYTICAL METHODS FOR MULTYLEVELEMBEDDING IN BMP-IMAGES
Minaeva Tamara, Voloshina Natalia, Bezzateev Sergey 230

APPLICATION OF THE PYTHON PROGRAMMING LANGUAGE FOR NETWORK SECURITY TOOLS DEVELOPMENT
Nikitin Andrey, Moskvin Dmitry ... 235

ENVIRONMENTAL CONTROL AND DEVELOPMENT OF MODELS OF POPULATION GROWTH
Pavlova Svetlana ... 236

MODELINGOFTHE COMPLEX MACHINES DURING THEIR ACCEPTANCE TESTING
Pervukhina Elena, Osipov Konstantin, Golikova Victoria ... 240

METHODS OF DATA EXTRACTIONFROM ISOLATED MACHINES
Romanov Alexander ... 245

BLOCKCHAIN-TECHNOLOGIES PROVIDINGINFORMATION SECURITY AT THEDECISION MAKING TO CONTROL THE SOCIO-ECONOMIC SYSTEMS
Tokarev Aleksey ... 246

INTEGRATED SYSTEM OF ENGINEERING AND TECHNICAL PROTECTION OF THE MANAGER'S OFFICE. THE EFFECTIVENESS OF THE WORK OF INFORMATION SECURITY DEVICES ON THE EXAMPLE OF AN INTEGRATED SYSTEM OF ENGINEERING AND TECHNICAL PROTECTION OF THE MANAGER'S OFFICE
Fayazov Kobiljon ... 247

APPLICATION OF DYNAMIC MODEL OF CONFRONTATION FOR MANAGEMENT OF INFORMATION SYSTEMS SECURITY
Shishkin Vladimir, Kolesnikov Konstantin ... 251

MODEL OF DISCOVERY AN INSIDE ATTACKER BASED ON BIG DATA TECHNOLOGIES
UshakovIgor, Kotenko Igor ... 253

SECURITY DATABASES FORA CORPORATIVE NETWORK: IMPLEMENTING SQL AND NoSQL TECHNOLOGIES
Ushakov Igor, Kotenko Igor ... 254

INFLUENCE OF DATA CHANGES DYNAMICS IN THE PROCESS OF SECURITY EVENTS CORRELATION
Fedorchenko Andrey, Kotenko Igor ... 256

SECURITY EVENT FORMATS IN LOGGING SYSTEM OF OS WINDOWS
Fedorchenko Andrey,Chechulin Andrey,Doynikova Elena ... 258

SECURITY THREATS IN SOCIAL NETWORKS AND PROTECTION FROM INFORMATION
Pronoza Anton, Chechulin Andrey, Komashinsky Nikolay ... 259

AUTOMATIC DETECTION OF DIFFERENCE BETWEEN THE INTERESTS OF SOCIAL NETWORK USERS OF DEPENDING ON THEIR COGNITIVE FUNCTIONS
Pronoza Anton, Pronoza Ekaterina, Chechulin Andrey, Kotenko Igor ... 261

MODERN MEANS OF INFORMATION PROTECTION ... 264

PENETRATION TESTING OF DATA PROTECTION SUITE VGATE R2
Borodin Mihail, Borodina Polina ... 264

IDENTIFICATION OF MOVING OBJECTS IN DISTRIBUTED INFORMATION-MEASURING SYSTEMS
Zakasovskaya Elena, Tarasov Valentin, Nyutenko Sergei ... 269

MODELINGOF THE COMPLEX MACHINES DURING THEIR ACCEPTANCE TESTING
Pervukhina Elena, Osipov Konstantin, Golikova Victoria ... 273

DESIGN OF TREE-BASED SERIAL DATA STORAGES WITH INCLUDED DIGITAL SIGNATURES
Romanova Yuliya, Yanyushkin Konstantin ... 277

LEGAL ASPECTS OF INFORMATIZATION AND INFORMATION SECURITY ... 281

THE POTENTIAL OF THE MEDIA IN TRANSFORMATION OF POLITICAL CONSCIOUSNESS OF THE SOCIETIES OF THE EAEU
Gaishun Alexander ... 281

COUNTERING EXTREMISM IN THE INTERNET NETWORK IN THE EUROPEAN UNION AND THE RUSSIAN FEDERATION
Dolgoshein Petr ... 283

SPIRITUALLY-MORAL ASPECTS OF INFORMATIVE SAFETY
Iventiev Sergei ... 285

INFORMATION-ECONOMIC SECURITY 289

THE THEORY OF DECISION-MAKING IN MATTERS OF ECONOMIC SECURITY ENTITY
Bolshakova Lyudmila, Dashkov Andrey, Yakovleva Natalia 289

ON THE PERSPECTIVES OF APPLICATION OF SPATIAL-TIME CODING IN THE RADIOLINIAS OF THE NAVY
Tipikin Alexey, Pooh Gennady 291

STRATEGIES OF INFORMATION TECHNOLOGIES DEVELOPMENT IN REGIONAL ECONOMIC SYSTEMS, BASED ON DIFFERENT TYPES OF REACTIONS TO THE CHALLENGES OF THE EXTERNAL ENVIRONMENT
Titovets Alisa 293

PREPARATION AND RETRAINING OF IT SPECIALISTS 296

REALIZATION OF COMPETENCE-BASED APPROACH WHEN FORMING POOP OF NEW GENERATION ON THE EXAMPLE OF THE LABORATORY PRACTICAL WORK «SAFETY OF INFORMATION SYSTEMS»
Barabash Pavel, Panasenko Mikhail 296

PROFESSIONAL AND EDUCATIONAL STANDARDS AS THE BASIS OF THE INTERACTION AMONG EDUCATION, SCIENCE AND INDUSTRY EMPLOYERS IN COMPETENCE-ORIENTED TRAINING OF SPECIALISTS IN THE SPHERE OF INFORMATION SECURITY IN TECHNICAL UNIVERSITY
Zhigadlo Anna, Odinokaya Mary 299

THE ROLE OF PROFESSIONALAND EDUCATIONAL STANDARDSINTHESPHERE OFINFORMATIONTECHNOLOGIES
Zhigadlo Nadezhda 300

DISTANCE EDUCATION AS OPERATIONALLY DIDACTIC FORM OF PROFESSIONAL DEVELOPMENT OF PEDAGOGICAL STAFF IN CONTINUING EDUCATION ADULTS
Katkova Irina, Cecarenko Olga 301

THE CONCEPT OF SOCIAL ADAPTATION OF EMPLOYEES OF POWER MINISTRIES AND DEPARTMENTS, RETIRED
Mikhalev Yuri., Hlyupin Vladimir 306

THE METHODS OF PROVIDING INFORMATION SEQURITY OF THE UNIVERSITY ELECTRONIC DATAINFORMATION AND EDUCATIONAL ENVIRONMENT
Sokolov Sergey, Nyrkov Anatoliy, Kovalnogova Nadegda, Mamunts David, Pastushok Elena 309

PEDAGOGICAL AND TECHNOLOGICAL ASPECTS OF THE USE OF COMPUTER-BASED TESTING AT DIFFERENT STAGES OF LEARNING THE DISCIPLINE
Titova Yuliayna 312

INFORMATION TECHNOLOGIES ON TRANSPORT 319

SCIENTIFIC AND METHODOLOGICAL APPROACHES TO ENSURE SAFETY OF INFORMATION SYSTEMS IN TRANSPORT
Belov Andrey, Barabanov Vladimir 319

THE TOP-10 INFORMATION SECURITY THREATS IN VANET: ANALYTICALSURVEY
Buinevich Mikhail, Stolyarova Ekaterina, Khoroshenko Sergei, Shiryaev Denis, Vladyko Andrei 323

INFORMATION SECURITY OF TRAFFIC OF SHIPS
Bukharmetov Maxim, Nyrkov Anatoli 328

USING MATHEMATICAL MODELS IN THE ASSESMENT OF THE EFFICIENCY WORK OF OIL WELLS
Anastasiya Virstyuk, Viktoria Mikshina, Alik Elmendeev 329

INFORMATION SECURITY IN MANAGEMENT OF CITY TRANSPORT, AS THE ELEMENT OF IMPLEMENTATION OF THE CONCEPT OF "THE CLEVER CITY"
Zhigadlo Valentin 331

PROBLEMS OF INFORMATION SECURITY OF MARITIME TRANSPORT SYSTEMS
Goloskokov Konstantin, Chirkova Marina 332

FLASH-MOB AS A PROTEST TECHNOLOGY IN THE POLITICAL MOVEMENT (ON THE EXAMPLE OF UKRAINE)
Degtiareva Olga 334

INFORMATION SECURITY WHEN USING AN AUTOMOBILE AUTOPILOT
Kucherovskaya Olesya ... 337

ANALYSIS OF MODERNTHREATS AND THEIR METHODS OF PENETRATION INTO THE SYSTEM
Lukin Evgeny, Prokopovich Maxim ... 339

CAR CLUSTER SANKT PETERSBURG
Polyakov Dmitry ... 342

USE OF CONSUMER CONTROL IN INTELLIGENT ROAD SAFETY SYSTEMS
Seliverstov Yaroslav, Seliverstov Svyatoslav ... 344

INFORMATION TECHNOLOGIES OF MANAGEMENT OF OBJECTS OF MARINE TECHNIQUE AND SEA INFRASTRUCTURE ... 348

THE PROBLEM OF CREATING AN IT MANAGEMENT STRUGGLE FOR SURVIVABILITY OF OMT IN A SECURE EXECUTION AND PROMISING WAYS OF THEIR SOLUTION
Alekseev Anatoly, Solovyov Sergei, Boronenkov Ivan, Turkin Igor, Moskalenko Vasily, Musatenko Roman ... 348

REGRESSION ANALYSIS OF THE DYNAMICS OF 10 YEARS OF HACKING AND INFORMATION INCIDENTS
Antsiferov Alexander ... 350

ANALYSIS OF VULNERABILITY OF SERVICES AUTHORIZATION AND POSSIBILITIES OF THEIR IMPROVEMENT
Biryukova Aleksandra ... 352

VULNERABILITY, THREATS, AND ASSESSMENT OF DEFINITION OF SERVICE DATA OUTLOOK
Karmazin Zhan ... 353

INFORMATION SECURITY IN THE MARITIME SECTOR OF THE EUROPEAN UNION
Kolesnikova Marina ... 354

THE FEATURES OF THE DEVELOPMENT OF INFORMATION SUPPORT SYSTEMS OF FIGHT FOR SURVIVABILITY OF SUBMARINE WITH THE INFORMATION SECURITY REQUIREMENTS
Levoeva Inga, Mudrova Alena ... 358

WEB APPLICATION SECURITY AND VULNERABILITIES
Povecherov Dmitriy ... 360

PRACTICE OF TESTING AND POSSIBILITY OF DEVELOPMENT OF TECHNOLOGIES OF PC «FORTINET»
Podgornova Valeriya ... 361

VISUALIZED LOGICAL-PROBABILISTIC MODELS OF STRUCTURALLY COMPLEX TECHNICAL SYSTEMS ... 362

PoleninVladimir, Sushchenkov Dmitry ... 362

METHODOLOGY FOR CONSTRUCTION OF LOGIC-PROBABILISTIC MODELS OF STRUCTURALLY COMPLEX TECHNICAL SYSTEMS FOR RISK ASSESSMENT AND SAFETY OF THEIR FUNCTIONING
Polenin Vladimir, Potekhin Alexander ... 364

COMPUTER VIRUSES: HISTORY, CLASSIFICATION, OPPOSITION
Tsygankov Ilya ... 369

INFORMATION TECHNOLOGIES IN ECOLOGY ... 371

ECLIPSING REMOTE SENSING OF THE EARTH'S UPPER ATMOSPHERE FROM MANNED SPACECRAFT: OBTAINING AND SAVING THE INFORMATION
Buznikov Anatoliy ... 371

A CONCEPT OF INTRALABORATORY CONTROL OF BIOTESTING RESULTS IN ECOANALYTICAL LABORATORIES FOR ENHANCEMENT OF INFORMATION SECURITY OF CONTROL OF WATER MEDIUM TOXICITY
Velichko Anna ... 373

LOCAL FACTORS OF GLOBAL CLIMATE CHANGING (ANALISYS OF ATMOSPHERE MONITORING SYSTEMS IN MEGALOPOLISES)
Viktorov Sergey, Labzovskiy Lev ... 375

MATHEMATICAL MODELS IN THE ANALYSES OF THE EFFICIENCY WORK OF OIL WELLS
Virstyuk Anastasiya, Mikshina Viktoria ... 376

REMOTE SENSING OF COASTAL WATERS OF THE SEA OF OKHOTSK: A COMPARISON OF SPECTROMETRIC AND LIDAR METHODS
Goryainov Viktor, Buznikov Anatoliy, Chernook Vladimir ... 380

INCREASING EFFICIENCY OF THIN-FILM SOLAR MODULES TO PROVIDE INFORMATIONAL AND ECOLOGIC SAFETY
Gulkov Valeriy ... 381

METHOD OF RESTORING THE WIND PROFILE DUE TO SPECTRE WIDTH ESTIMATION OF THE RADAR SIGNAL
Denisenkov Dmitriy, Zhukov Vladimir, Shukin Georgiy ... 382

INFORMATION AND OPERATIONAL ENVIRONMENTAL SAFETY ACTIVITIES LAW ENFORCEMENT AGENCIES AND BRANCHES OF THE RUSSIAN ECONOMY
Doronin Aleksandr, Shchukin Georgiy, Petrochenko Vyacheslav, Kozlova Natalia, Timoshchuk Aleksandr, Shmalko Svetlana ... 384

FEATURES OF THE SOLUTION OF PROBLEMS OF ECOLOGICAL SAFETY OF THE MEGALOPOLIS
ZhigadloValentin ... 387

PROBLEMS OF OBTAINING INFORMATION ON SAFETY OF THE WATER ENVIRONMENT BY BIOTECHING ON THE BASIS OF EXISTING REGULATIONS
Zakharov Igor ... 388

RADAR METHODS FOR MEASUREMENT OF HYDROGRAPHIC PARAMETERS OF SEA
Orandarenko Elena ... 389

ESTIMATION OF STRUCTURAL MEANINGFULNESSOF ELEMENTS IS IN INFORMATIVE SYSTEMS OF ECOLOGICAL MONITORING
Ryabovaya Valentina ... 393

FLEXIBLE ORGANIC SOLAR CELLS BASED ON A SYSTEM OF «PHTHALOCYANINE/FULLERENE»
Tarasov Sergey ... 397

INFORMATION SECURITY OF CYBERPHYSICAL SYSTEMS ... 399

PROTECTION OF INFORMATION IN AUTOMATED MULTI-LEVEL SYSTEM PROBLEMS
Bondarenko Igor, Shimanchuk Sergey ... 399

ANALYSIS OF THE METHOD OF BIOMETRIC AUTHENTICATION FOR THE PAYPASS SYSTEM
Davydov Vadim ... 402

INFORMATION SECURITY AND CYBER-STABILITY OF THE DIGITAL ECONOMY AND DIGITAL PRODUCTION
Zegzhda Peter, Zegzhda Dmitry ... 406

SOCIAL ENGINEERING. PHISHING AND METHODS OF COUNTERING IT
Ilchenko Lydia, Uvarov Roman, Zaytsev Svyatoslav ... 407

DATA VISUALIZATION MODELS USAGE IN DLP SYSTEMS
Kolomeec Maxim ... 411

DETECTION OF ANOMALIES IN BEGAVIOR OF PROGRAM PROCESS USING MASHINE LEARNING
Labutina Eugenia ... 413

THE APPROACH TO DESIGN OFSECURE SYSTEMSBASED ON EMBEDDED DEVICES
Levshun Dmitry ... 415

ORGANIZATION OF COLLECTIVE MANAGEMENTBASED ON UNMANNED AERIAL VEHICLES
Marinenkov Egor, Shuvaev Alexander ... 417

INVESTIGATION OF PROTECTION OF CONTROL SYSTEMSMOBILE DEVICES
Medvedev Mikhail, Bezhan Roman, Arustamov Sergey ... 419

ASSESSMENTOF RISKS: COMPARATIVE ANALYSIS OF APPROACHES AND METHODOLOGIES
Meleshko Aleksei, Chumak Evgeny, Savkov Sergey ... 420

APPLICATION OF NEURAL NETWORKS IN THE FIELD OF INFORMATION SECURITY
Orlov Ivan ... 423

ANALYSIS OF THE BEHAVIOR PROPERTIES OF THE SUBJECT WITH AUTHENTICATION ON THE EXAMPLE OF MANUAL SIGNATURE USING THE ACCELEROMETER
Rudavin Nikolay ... 426

METHODS AND TOOLS OF THE AUDIT OF NETWORK SECURITY
Sadikova Anastasia, Titova Yulia, Savkov Sergei 430

INCREASE OF ACCURACY OF STEGOANALYSIS METHODS BY OPTIMIZING PARAMETERS OF WAVELET-TRANSFORMATION
Sivachev Alexey, Mikhailichenko Olga 435

THE PROBLEM OF ANONYMITY IN THE INTERNET NETWORK. COMPARISON OF METHODS OF USER ANONYMIZATION
Titova Yulia, Sadikova Anastasia, Savkov Sergei 437

YOUTH SCIENTIFIC SCHOOL: SAFE INFORMATION TECHNOLOGIES 442

APPLICATION OF MACHINE LEARNING IN DEEP TRAFFIC ANALYSIS
Alexandrovna Ekaterina 442

ENSURING INFORMATION SAFETY OF AUTOMATED SYSTEMS OF TECHNOLOGICAL PROCESS CONTROL
Bondareva Anastasia, Goman Elena 444

COMPARATIVE ANALYSIS OF FINANCIAL TRANSACTIONS SECURITY USING CONTACTLESS PAYMENT TECHNOLOGIES
Ganchikova Yulia, Kurysheva Alena 445

OVERVIEWODLPSYSTEMS
Gerzen Dmitry, Stafeev Aleksey, Serdyukov Nikita 446

PROSPECTS OF ONE-TIME PAD USAGE FOR PROTECTION OFUNMANNED AERIAL VEHICLE DATASTREAMS
Grozov Vladimir 451

MAJOR THREATS OF INFORMATION SAFETY OF THE WAREHOUSE, WORKING UNDER THE MANAGEMENT OF THE WMS-SYSTEM
Guba Evgeny 452

SIMULATION OF THE HUMAN BODY TO SUPPORT MEDICAL DECISIONS
Gubin Alexander, Ignatiev Mikhail, Katerina Tatiana, Krasnikov Andrey 454

USING BIG CODE FOR ASSESS OF SOFTWARE RELIABILITY
Zakoldaev Danil, Rimsha Andrei, Iuganson Andrei 455

PARTICULAR QUALITIESOF CONSTRUCTION OF INFORMATION PROTECTION SYSTEM IN INTELLECTUAL SYSTEMS OF GROUND CITY PASSENGER TRANSPORT
Ilchenko Lydia, Zaytsev Svyatoslav 458

SOCIAL ENGINEERING AS A METHOD OF UNAUTHORIZED ACCESS TO THE INFORMATION CONCERNING THE TRADE SECRET
Kizryakova Anastassiya, Solodovnikov Vladislav 462

METHODS OF SOCIAL ENGINEERING AS A WAY TO ACCESS INFORMATION OF LIMITED ACCESS
Kizryakova Anastassiya, Solodovnikov Vladislav 465

APPLICATION OF NEW VISUALIZATION MODELS TO IMPROVE THE EFFECTIVENESS OF USER-MADE SOLUTIONS
Kolomeec Maxim, Chechulin Andrey 466

WIRELESS SENSOR NETWORK ATTACK IDENTIFICATION IN THE BASIS OF NETWORK BEHAVIOUR ANALISIS
Korzhuk Victoria 468

ANALYSIS OF ERP-SYSTEMS SECURITY. GENERAL APPROACH TO ANALYSIS
Krivdyuk Nadezhda 469

COMPARATIVE ANALYSIS OF FINANCIAL TRANSACTIONS SECURITY USING ELECTRONIC PAYMENT SYSTEMS
Kurysheva Alena, Ganchikova Yulia 470

METHODOLOGY FOR FORMING SECURITY REQUIREMENTS TO ECM SYSTEMS
Leyfer Anastasiya 471

SYSTEM OF DATA COLLECTION AND ANALYSIS FOR THE STUDY OF THE UNIQUE BEHAVIOR SIGNS OF MOBILE DEVICEUSERS
Leyfer Kirill 474

ANALYSIS OF EXISTING SENSORS FOR DETECTING THE ATTEMPTS OF UNAUTHORIZED ACCESS TO PROTECTED INFORMATION
Lisetskaya Kristina ... 476

THE ANALYSIS OF QUESTIONS OF INFORMATION SECURITY ON THE WIRELESS SENSOR NETWORKS OF MEDICAL ASSIGNMENT
Losev Roman, Ruchkan Alexander ... 477

THE REVIEW OF EXISTING DECISIONS OF INFORMATION SAFETY MONITORING SYSTEMS
Lyamzina Alisa, Korzhuk Victoria ... 478

INVESTIGATION OF THE APPLICABILITY OF THE METHOD OF EVENT BUSH IN THE FIELD OF INFORMATION SECURITY
Naumov Andrey, Popov Ilya ... 479

ACCESS CONTROL AND MONITORING SYSTEM, FOR EXAMPLE, A HIGHER EDUCATION INSTITUTION
Sazonov Anton,Nemchenko Aleksey ... 480

METHOD OF CONDUCTING INTERNAL AUDIT OF INFORMATION SECURITY OF ORGANIZATION
Sozinova Ekaterina ... 483

THE PROBLEM OF NON-COMPLIANCE OF MEDICAL ORGANIZATIONS' INFROMATION SECURITY SERVICES WITH MODERN REQUIREMENTS OF PHYSICAL PROTECTION MEASURES
Fedorova Alyona, Alekseev Dmitriy ... 484

METHOD OF PRELIMINARY PROCESSING OF GRAPHIC OBJECTS IN THE VIDEO SEQUENCE FOR IDENTIFICATION
Shevchenko Denis ... 485

LOCATING VIOLATION OF SAFE SOFTWARE RESOURCE USE IN A PROGRAM
Tcvetkov Lavrentii, Spivak Anton ... 489

MODEL OF DETECTION OF DESTRUCTIVE IMPACT ON MULTI-AGENT ROBOTIC SYSTEMS
Iureva Radda, Timko Andrey, KomarovIgor ... 491

YOUTH SCIENTIFIC SCHOOL: INFORMATION TECHNOLOGIES AND PROBLEMS OF SUSTAINABLE DEVELOPMENT ... 493

BUSINESS GAME «MODELING CITIES AS COMPLEX SELF-ORGANIZING HUMAN-MACHINE SYSTEMS»
Ignatyev Mikhail ... 493

ABOUT THE CONTROL OF ROBOTIC SYSTEMS IN A THREE-DIMENSIONAL SPAC
Ignatyev Mikhail, Catermina Tatyana, Lipinski Jan,Nenashev Vadim ... 495

INTENTIONAL ARTIFICIAL INTELLIGENCE ON THE BASIS OF THE LINGUO-COMBINATORIAL SIMULATION
Ignatyev Mikhail ... 496

MODELREPRESENTATIONOFPROGRAMMABLE LOGIC DEVICES IN REVERSE ENGINEERING TASKS
Bykov Andrey, Demchenko Oleg, Usatiy Vadim ... 497

THE TIME ARROW AND THE IRREVERSIBILITY OF PROCESSES IN COMPLEX DYNAMICAL SYSTEMS
Ostreykovsky Vladislav, Muraviov Igor,Shevchenko Elena ... 501

APPROACHES TO ASSESSING THE RELIABILITY OF COMPLEX SYSTEMS
Svezhentsev Igor ... 505

CONTENTS ... 522