САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 6

Санкт-Петербург
2018

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 6

Санкт-Петербург
2018

http://spoisu.ru

УДК (002:681):338.98

Р32

Региональная информатика и информационная безопасность.

Р32 Сборник трудов. Выпуск 6 / СПОИСУ. – СПб., 2018. – 266 с.

ISBN 978-5-907050-54-9

Сборник статей охватывает широкий круг направлений Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России» и Санкт-Петербургской международной конференции «Региональная информатика», проведенных при поддержке Правительства Санкт-Петербурга: Государственная политика в сфере информатизации и информационной безопасности; Теоретические проблемы информатики и информатизации; Информационная безопасность; Информационно-психологические и правовые аспекты информационной безопасности; Информационные технологии в экономике; Информационные технологии на транспорте; Информационные технологии в образовании; Информационные технологии в медицине и здравоохранении; Информационные технологии управления объектами морской техники и морской инфраструктуры; Молодежная научная школа безопасные информационные технологии; Молодежная научная школа информационные технологи математического моделирования.

Предназначен для широкого круга руководителей и специалистов органов государственной власти и местного самоуправления, промышленности, науки, образования, бизнеса, аспирантов и студентов высших учебных заведений, 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 12.10.2018. Формат 60x84⅛. Бумага офсетная.
Печать – цифровая печать. Усл. печ. л. 30,9. Тираж 500 экз. Заказ № 1486
Отпечатано в ООО «Политехника Сервис»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-907050-54-9

© Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления (СПОИСУ), 2018 г.
© Авторы, 2018 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 6

St. Petersburg

2018

http://spoisu.ru

http://spoisu.ru

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В СФЕРЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 681.518

КВАЛИМЕТРИЧЕСКАЯ ПАРАДИГМА ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЩЕСТВА

Алексеев Анатолий Владимирович
Институт автоматизации процессов борьбы за живучесть корабля, судна
Ленинский пр., 101, Санкт-Петербург, 198262, Россия
e-mail: iapbgks@bk.ru

Аннотация. На основе анализа тенденций моделирования факторов воздействия на развитие Государства и Общества, включая положения национальной программы цифровой экономики, предложена квалиметрическая парадигма и модель цифровой трансформации Государства и Общества, отличающаяся обоснованием, прогнозированием и оптимизацией управленческих решений во всех сферах деятельности за счет квалиметрически обеспеченных количественных данных об уровне качества управления, их информационно-прозрачного мониторинга и контроля. Это позволяет количественно обосновывать стратегию развития Государства и Общества, выбирать лучший из возможных (оптимальный) путь технологического и социально-экономического развития за счет их цифровой трансформации. Приведен пример технологического обеспечения и показана особая роль цифровой трансформации Государства и Общества на базе количественного анализа качества управления, факторов конкурентной способности национальной продукции и услуг, системного мониторинга, прогнозировании и управлении развитием в процессе цифровой трансформации Государства и Общества в целом.

Ключевые слова: цифровая экономика; качество управления; парадигма; квалиметрия; модель конкурентной способности; цифровая трансформация.

QUALITATIVE PARADIGM MODEL AND THE DIGITAL TRANSFORMATION OF SOCIETY

Alekseev Anatoly
Institute of automation of processes of struggle for survivability of the ship, vessel
101 Leninsky Av., St. Petersburg 198262, Russia
e-mail: iapbgks@bk.ru

Abstract. On the basis of the analysis of trends in modeling factors influencing the development of the State and Society, including the provisions of the national program of the digital economy, the proposed qualimetric paradigm and model of digital transformation of the State and Society, characterized by justification, forecasting and optimization of management decisions in all spheres of activity due to the qualimetrically provided quantitative data on the level of quality of management, their information-transparent monitoring and control. This allows us to quantitatively justify the strategy of development of the State and Society, to choose the best possible (optimal) way of technological and socio-economic development through their digital transformation. The example of technological support is given and the special role of digital transformation of the State and Society on the basis of the quantitative analysis of quality of management, factors of competitive ability of national production and services, system monitoring, forecasting and management of development in the process of digital transformation of the State and Society as a whole is shown.

Keywords: digital economy; quality of management; paradigm; qualimetry; competitive ability model; digital transformation.

1. Актуальность темы. Среди актуальных для исследования факторов воздействия на развитие Государства и Общества (ФРГО), их технологического, социального и межгосударственного развития в целом, влияния на возможность вести успешное конкурентное противоборство на мировом рынке [1-3] наибольшее влияние оказывают инновационные, инвестиционные и финансовые факторы деятельности Государства и Общества. При этом основными системными ФРГО, как правило, являются:

– качество товаров и услуг (КТУ), предоставляемых Обществу производителями, определяемое действующими в Государстве стандартами, нормами и рекомендациями заказчиков и потребителей, а также фактическими условиями конкуренции на внутреннем и мировом (межгосударственном, глобальном) рынках;

– система экономических показателей, формирующих себестоимость и цену товаров и/или услуг (СТУ);

– системные (включая организационно-экономические) показатели соответствия государственных программ развития Общества его экономическому потенциалу (СПС);

– конкурентная способность Государства и Общества (КСГ) на мировом (глобальном) рынке;

– финансово-экономическое состояние Государства и Общества (ФЭС);
– репутация Государства на мировом (межгосударственном, глобальном) рынке товаров и услуг (РГР);
– другие ФРГО, в том числе неизвестные (ДФР).

При этом раздельный анализ факторов развития Общества и Государства (как формы организации Общества), позволяет оценивать степень соответствия интересов и прогрессивности (регрессивности) развития Общества его государственной форме устройства. Это, в свою очередь, позволяет с единой научно-методологической позиции оценивать степень гармонизации отношений Общества и Государства, вырабатывать рекомендации по совершенствованию и оптимизации форм государственного устройства и деятельности, обоснованно определять приоритетные направления развития Общества и Государства.

На рис. 1 приведен вариант графической модели ФРГО, позволяющий в структурированном виде представлять и анализировать соответствующие взаимосвязи факторов развития и их свойства.

Рис.1. Вариант классификации факторов развития Государства и Общества

2. Проблема квалиметрической оценки влияния ФРГО. Многообразие, разнородность и динамика взаимосвязей, приведенных в данной упрощенной модели ФРГО, прежде всего, указывает на актуальность и принципиальную необходимость их системного исследования, модельного представления, научно обоснованного ретроспективного анализа и синтеза перспективных вариантов развития с формированием соответствующих ожидаемых и планируемых качественных и, безусловно, количественных показателей развития.

3. Особенности и требования к анализу ФРГО. В этом контексте первостепенное значение и актуальность имеет развитие научно обоснованных парадигм, концепций и моделей развития Общества и Государства. При этом, безусловно, лидирующая роль в этом специфичном для науки процессе должна принадлежать исключительно ученым и соответствующим специалистам, профессионально владеющим технологиями системного моделирования, системного анализа и синтеза, методами численного эксперимента.

Причем, различные концептуальные подходы должны беспристрастно фиксироваться в базе данных и знаний (БДЗ) с соответствующей квалифицированной количественной оценкой качества, как меры соответствия предназначению. И, обязательно, в сравнительном (сопоставительном, ранжированном) аспекте. Это позволит, с одной стороны, сопоставлять перспективность парадигм, концепций, программ развития, а, с другой стороны, давать авторам повод и тему для развития идей, и наращивания их качественного уровня.

Еще более значимым следует считать при этом обеспечение принципа «информационной прозрачности» каждого из концептуальных подходов, их «исходного» толкования (содержания в авторской редакции) и, даже, авторской принадлежности, в том числе для систематизации данных и парадигм при их развитии.

Это обеспечит состоятельность каждого подхода, включая возможность публичного отстаивания авторами самодостаточности предлагаемого подхода в условиях любых возможных и плюралистически допустимых альтернативных мнений, что на этапе становления парадигм и концепций будет только полезным.

Не вызывает сомнения, что в этих условиях «научно-образовательное сообщество» [13] должно располагать, а Общество и Государство должно признать и доверить возможность сравнивать предлагаемые концепции с использованием соответствующих квалиметрических моделей, методик и аппарата. Например, на основе соответствующих сертифицированных программных комплексов с соответствующими тестовыми вариантами и матрицами модельных индексов, БДЗ по каждому из альтернативных вариантов парадигм, концепций и т.д.

Как известно, без подобных процедур и количественных сравнительных оценок анализ валидности и верификация предлагаемых парадигм (как научных идей) и концепций, а, тем более, их обсуждение в Обществе принципиально не должно быть возможным. Использование подобного «подхода» аналогично использованию «птичьего языка» (по содержанию - типа «чик-чирик»), т.е. по существу на неопределенном количественно уровне, с использованием голословных утверждений, «давления авторитетами» и т.п.

4. Возможность реализации требований. Следует отметить, что необходимые научно-методические инструменты сегодня имеются (например, включая [3-7]), а Государству и Обществу остается только определиться с выбором «наиболее достойного» из них и обеспечить публичность своего выбора. Причем, наиболее перспективным, по нашему мнению, следует считать в этой задаче использование так называемого [8-9] полимодельного принципа и алгоритма выбора, основанных на одновременном использовании при одинаковых исходных данных нескольких научно-методических аппаратов с соответствующими средствами программной поддержки принятия решений и едиными регламентами регистрации в БДЗ, системного анализа и т.п.

В этом контексте роль Государства и Общества в создании необходимых условий для цифровой трансформации Общества [13] и обеспечения гармонического развития с использованием научного и социального потенциалов будет, по нашему мнению, только повышаться. А совершенствование на основе этой парадигмы процессов управления приобретёт «естественный» вид и создаст доверительную среду коллективного поиска и, можно сказать, коллективного когнитивного творчества. При этом, возможная социальная напряженность перейдет из формы противостояния и, даже, противоборства мнений в форму консолидации усилий и концентрации интеллектуального потенциала Общества на общих направлениях, перехода от конкурентного противоборства к конкурентной «лояльности», привлекательности и приоритетности методического развития.

Однако, анализ практик оценки эффективности инвестиционных проектов и их привлекательности показывает, что сегодня показатели конкурентной способности товаров и услуг (КС), а, тем более, КТУ, КСГ, как функции КТУ, СТУ, СПС, ФЭС, РГР, ДФР, при этом учитываются в ограниченном объёме (не системно целостно), либо практически не учитываются. В первую очередь, даже показателей КТУ с учетом фактической специфики многокритериального и полимодельного оценивания качества товаров и/или услуг.

Более того, ожидается даже некоторая взаимная нейтрализация таких весьма значимых и важных сегодня системных ФРГО, деятельности предприятий и обеспечения жизненного цикла выпускаемой им продукции и услуг (ЖЦП), как [1, 2, 3]:

– позитивные и негативные субъективные свойства участников создания, сбыта и потребления продукции предприятия, именуемые на качественном уровне сегодня упрощенно «человеческим фактором» (ЧФ, ССУ);

– инфраструктурные факторы предприятия, сбытчиков и потребителей продукции предприятия, которые условно назовем «инфраструктурными факторами жизненного цикла продукции» (ИФП), включая местоположение пунктов производства, сбыта и потребления продукции, имиджевые, репутационные и т.п. факторы;

– другие менее значимые и/или неучтенные факторы деятельности предприятия (ДФП).

5. Угрозы и проблема качества управления ФРГО. Наращивание даже вербального описания ФРГО при моделировании КС продукции базовых предприятий в сочетании с резким возрастанием объёма математического описания модели КС, КСГ приводит многих исследователей и, даже, заказчиков к отказу от решения задачи числового моделирования (проблема 1) в связи с резким возрастанием её сложности, появлением сомнений в части ожидаемой практической значимости подобных моделей (проблема 2), в том числе по причине «сомнительности» получения адекватных исходных данных и знаний [3-4] (проблема 3).

Это в результате приводит к кажущейся неизбежности использования «ручного» метода управления с не менее сомнительной «ожидаемой эффективностью» (проблема 4). Тем более, например, для современных сложных организационно-технических эргатических систем с соответствующим скачком рисков неэффективных и ошибочных управленческих решений (проблема 5), что только усиливает влияние ЧФ, ССУ, а в целом ряде случаев порождает «нерешаемую проблему» коррупционного фактора (КФУ) [5-6] (проблема 6).

В свою очередь, эти и подобные факторы дополнительно и существенно ограничивают возможности инвестиционного анализа, синтеза и оптимизации проектных и управленческих решений, технологического развития предприятий и выпускаемой ими продукции (товаров и/или услуг) [7], а, тем более, ФРГО (проблема 7).

6. Пути решения проблемы качества управления ФРГО. Практически безальтернативным путем решения проблемы качества управления ФРГО следует считать активизацию научного обоснования и интенсивного развития методологии анализа и синтеза сложных эргатических систем (задача 1), включая такие её важнейшие аспекты, как КС предприятий и выпускаемой ими продукции, а также перспективность их развития (ПР), в целом КСГ [8-9], научная обоснованность и «информационная прозрачность» управления развитием предприятий и ключевых отраслей промышленности, а, тем более, Государства и Общества.

Безусловным вариантом реализации данной методологии должно быть использование сертифицированных программных средств интеллектуальной поддержки анализа и синтеза оптимальных вариантов программ развития КС предприятий и их продукции (задача 2), КСГ на основе лучших практик соответствующих инновационных решений при заданных (допустимых) объёмах инвестирования средств (задача 3).

7. Квалиметрическая парадигма цифровой трансформации Общества. В этом контексте рассмотрим новый квалиметрический подход и содержание квалиметрической парадигмы и модели «цифровой трансформации»

(цифровизации) Общества и Государства, весьма активно обсуждаемой сегодня в Обществе и его научно-образовательном сообществе [13]. Для этого, прежде всего, систематизируем основные положения, вкладываемые сегодня в это понятие, в форме предлагаемой аналитической таблицы.

Таблица 1

Систематизация основных понятий по проблеме цифровой экономики и трансформации Общества

Термин	Понятие, толкование термина
Цифровая экономика	Ключевой фактор производства во всех сферах социально-экономической деятельности, что повышает конкурентноспособность страны, качество жизни граждан, обеспечивает экономический рост и национальный суверенитет [13].
Цифровой сектор экономики	Сектор экономики (сектор электронной коммерции), состоящий из электронных товаров и услуг (в том числе услуг по выбору и заказу реальных товаров) [14].
Электронная экономика	Экономическая деятельность (цифровая, веб-, интернет-экономика), основанная на цифровых технологиях, связанная с электронным бизнесом и электронной коммерцией, и производимых и сбываемых ими электронными товарами и услугами. Расчёты за услуги и товары электронной экономики производятся зачастую электронными деньгами [14].
Цифровая трансформация	Интеграция цифровых технологий во все сферы бизнеса, которая приводит к фундаментальным изменениям в работе компании и отражается на ее взаимодействии с клиентами [16]. Предполагает смену руководства, разностороннее мышление, поощрение инноваций и новых бизнес-моделей, включая оцифровку активов и более широкое использование технологий. Также необходимо дополнять опыт сотрудников, клиентов, поставщиков, партнеров и акционеров компании [16]. Создание информационных систем различного назначения [11]. Процесс принятия решений на основе данных и их аналитики, минимизации человеческого фактора (редакция автора) [17]. С точки зрения экономики и психологии — это фундаментальный тренд. Мы пытаемся сделать наши решения более эффективными и рациональными [17]. Фундаментальный тренд и большой шаг к массовому увольнению [И. Игнатьев].
Цифровизация	Переход с аналоговой формы передачи информации на цифровую [16]. Системный подход к использованию цифровых ресурсов для повышения производительности труда, конкурентоспособности и экономического развития в целом [18].
Электронное правительство	Пакет технологий и набор сопутствующих организационных мер, нормативно-правового обеспечения для организации цифрового взаимодействия между органами государственной власти различных ветвей власти, гражданами, организациями и другими субъектами экономики. Предполагает эффективный способ предоставления информации о деятельности органов государственной власти, оказание государственных услуг гражданам, бизнесу, другим ветвям государственной власти и государственным чиновникам, при котором личное взаимодействие между государством и заявителем минимизировано и максимально используются возможности, предоставляемые информационными технологиями, мобильными технологиями и Интернетом [19].
Цифровая трансформация Государства и Общества (квалиметрическая парадигма трансформации Общества)	Социально-экономическое преобразование Государства и Общества на основе эффективного освоения и интеграции информационно-коммуникационных (цифровых) технологий во все сферы Государства и Общества с целью фундаментального (коренного) совершенствования и цифровизации экосистемы (социальной, окружающей и техногенной подсистем среды) за счет обоснования, прогнозирования и принятия эффективных и оптимальных управленческих решений во всех сферах деятельности на основе квалиметрически обеспеченных цифровых (количественных) данных об уровне качества управления, их информационно-прозрачного мониторинга и информационно-прозрачного контроля (отчетности) в интересах повышения и гарантированного обеспечения заданного (безопасно-комфортного) уровня качества жизни граждан и Общества в целом, повышения и гарантированного обеспечения конкурентноспособности и перспективности развития продукции и услуг на отраслевом, государственном и межгосударственном (глобальном, мировом) рынках как отдельных отраслей, так и экономики РФ в целом, а также повышения и гарантированного обеспечения правовой, социальной и фактической защищенности (безопасности) граждан, Общества, Государства, суверенитета РФ.

Следует отметить, что впервые парадигма электронной экономики появилась в последнем десятилетии XX века. В 1995 году Николас Негропонте использовал метафору о переходе от обработки атомов к обработке битов [15], отмечая о недостатке классических товаров в «физическом» воплощении (вес, сырьё, транспорт) и преимуществах новой экономики (отсутствие веса товаров, виртуальность, почти не нужное сырьё, мгновенное глобальное перемещение). Причем, именно как парадигма (от греч. Παράδειγμα - «пример, модель, образец» [https://ru.wikipedia.org/wiki/], совокупность фундаментальных научных установок, представлений и терминов, принимаемая и разделяемая научным сообществом и объединяющая большинство его членов, обеспечивающая преемственность развития науки и научного творчества).

А концепцию реализации этой парадигмы (от лат. conceptio - «система понимания», комплекс взглядов, связанных между собой и вытекающих один из другого; определённый способ понимания, трактовки каких-либо явлений; система путей решения задачи, определяющая стратегию действий) стали позже предлагать уже другие авторы, что, естественно, привело к некоторым несоответствиям исходного и производного толкований.

В этом контексте особую ценность приобретают взаимоувязанные и логически последовательные инновации в формате типа «тезаурус - парадигма – концепция – программа – технология – план». Это, к сожалению, встречается крайне редко. В этом аспекте, прежде всего, следует достаточно строго определить базовые понятия объекта инноваций типа «цифровая трансформация Общества (ЦТО)». Авторский вариант данного понятия и его парадигма приведен в нижней строке таблицы.

8. Пути развития и использования квалиметрической парадигмы ЦТО. На последующих этапах развития парадигмы конкретизация путей развития позволит методически однозначно определить и сформулировать такие важнейшие системные категории как цели, задачи и основные необходимые процессы ЦТО.

В свою очередь, это позволит логически последовательно перейти и сформулировать систему критериев оценивания качества процессов ЦТО. А при наличии соответствующих практических и статистических данных – определить граничные значения показателей качества решения задач (по частным, и групповым (характеризуют свойства объекта анализа) критериям и показателям), а также – граничные значения показателей достижения назначенных целей (по системным критериям и показателям).

Наличие названных цифровых данных позволяет на основе многовариантного (итерационного) использования автоматизированных систем моделирования качества экосистем и поддержки принятия управленческих решений, например, типа [3, 7-10], анализировать и синтезировать эффективные (рациональные) и оптимальные варианты архитектуры, функционала и алгоритмов функционирования любых по сложности экосистем. В том числе, например, объектов морской техники (типа судов, кораблей, морских платформ) и инфраструктуры (типа портов, транспортных путей, проектных и учебных организаций). Включая оценку уровней и динамику их цифровой трансформации, качества и эффективности самой цифровой трансформации, в том числе на соответствие задачам и требованиям, поставленных Правительством РФ и изложенных в Программе «Цифровая экономика Российской Федерации» [13].

9. Основные положения математического моделирования качества процессов ЦТО. В основу математической модели количественного анализа процессов ЦТО, обоснования стратегии социально-экономического развития целесообразно положить разработанные в последнее время перспективный метод, методологию, модель и алгоритм квалиметрической оценки [2 - 4, 9]. С учетом факторов конкурентной способности (КС) продукции и услуг Государства j-того типа $КС_j$ на основе гармонической модели агрегирования частных показателей качества (ЧПК) q_n с порядковым номером $n \in [1, N]$ в сравнении с аналогичным ЧПК ${q_n}^Б$ базового (исходного, опорного) объекта в агрегированный показатель КС в виде

$$КС_j = [\sum_{n=1}^{N}(w_n \times КП_n) \times \prod_{n=1}^{N} {КП_n}^{w_n}]^{0,5}, \quad (1)$$

$$КП_n = \left({q_n}/{q_n}_Б\right)^{z_n}, \quad (2)$$

где: $КП_n$ – конкурентное превосходство (КП) по ЧПК q_n;

w_n – индекс критериальной значимости (ИКЗ) n- того ЧПК;

z_n – индекс характера влияния ЧПК на агрегированный показатель КС, равный z_n=+1 при росте КС продукции и/или услуг при увеличении ЧПК и z_n=-1 – для случая снижения КС при увеличении ЧПК.

Данный метод предусматривает использование относительных шкал конкурентного превосходства $КП_n$, а также учет наиболее значимых с позиции инновационной и инженерно-технической целесообразности индексов корневой чувствительности (ИКЧ) вида

$$ИКЧ_{j,n} = (\Delta КС_j / КС_j)/(\frac{\Delta q_n}{q_n}), \quad (3)$$

что позволяет обоснованно синтезировать эффективные и оптимальные варианты архитектуры построения, функционала и алгоритмов функционирования продукции и услуг предприятий с номером j_{Opt} и Государства в целом в виде

$$j_{Opt} = ArgOpt\{ЛПР, Max(КС_j), Max(ИКЧ_{n,j}), \dots\}, \quad (4)$$

где в формальной записи (4) оператора поиска аргумента функционала оптимизации ArgOpt (оптимального номера варианта) запись ЛПР подчеркивает ту важную особенность решения

многокритериальных задач, которая сводится к тому, что решение об выборе оптимального решения при наличии подготовленных лицами, обосновывающими (ЛОР на основе компетенций, определяемых соответствующими знаниями, навыками, владением) и исполняющими (ЛИР на основе лучших практик и опыта) решения, массивов данных по максимальным значениям $КС_j$, $ИКЧ_j$ и другим принадлежит исключительно лицу, принимающему решения (ЛПР), на которого соответственно возлагается и должная ответственность, полномочия.

10. Специфические требования к информационно-аналитическому и интеллектуальному обеспечению управления ЦТО. Особая роль при реализации, приведенной и подобных парадигм, концепций и программ ЦТО, по нашему мнению, с учетом опыта создания и внедрения информационных технологий управления [3, 5-11] принадлежит технологиям типа СПРУ, СОТМУ [3, 4, 11, 20]. Эти технологии позволяют обеспечивать мониторинг динамики структурированных данных с их агрегированием и цифровой квалиметрической системной оценкой состояния сложных организационно-технических систем, аналогичных по структуре и функционалу названным выше. Вариант визуализации данных подобного мониторинга приведен на рис. 2 [20].

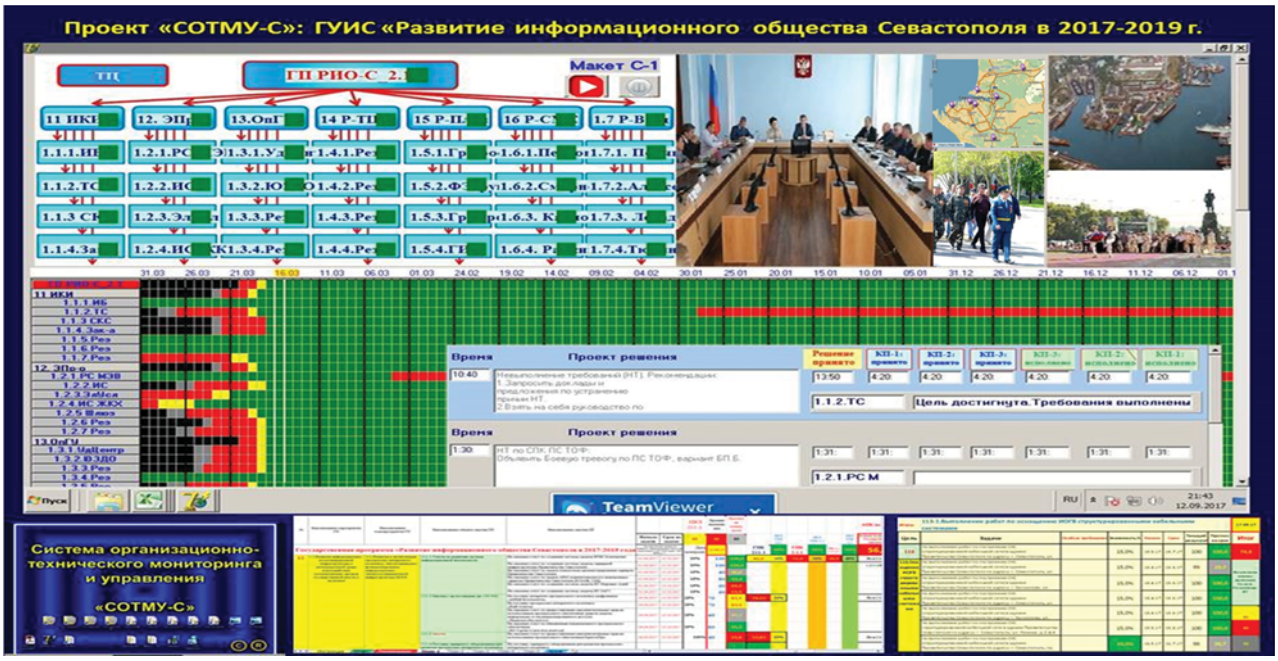


Рис.2. Пример технологии системной визуализации данных мониторинга Государственной программы «Развитие информационного общества Севастополя в 2017-2019 г.г.», применимый к задачам ЦТО

В целом, развитие и активное применение подобных технологий, по нашему мнению [21], позволяет в свете парадигмы и концепции ЦТО ставить задачу перехода к роботизации управления как средства гарантированной поддержки качества функционирования, в первую очередь, критически важных объектов, включая ОМТИ, с последующим их развитием и переходом к широкомасштабной цифровой трансформации Общества.

11. Выводы.

Подобный анализ КС и парадигма ЦТО должны производиться по всему множеству «управляемых» показателей, а задача оптимизации параметров продукции и услуг предприятия, отрасли, Государства и поиска предпочтительных вариантов его конкурентно способного развития является [20 - 21] итеративной, многокритериальной, полимодельной. И, безусловно, весьма сложной задачей числового моделирования, требующей привлечения широкого круга специалистов различных компетенций.

Вместе с тем, при обосновании стратегического развития именно подобный анализ позволяет интерпретировать тенденции развития и минимизировать риски управления, а тем более, заблаговременно вскрывать и своевременно исключать возможность неэффективных и ошибочных решений, в том числе упреждать неэффективность цифровой трансформации Государства и Общества. Тем самым, количественно обосновывать стратегию их развития, выбирать лучший их возможных (оптимальный) путь технологического и социально-экономического развития.

При этом, разработанные методы и средства моделирования ЦТО могут быть эффективно масштабироваться и использоваться при создании инструментальной среды поддержки проектного процесса и оптимизации проектных социально-экономических и государственных процессов и решений.

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. Субетто А.И., Алексеев А.В. Теория практики квалиметрического обеспечения развития морских автоматизированных систем / Актуальные проблемы морской энергетики: материалы седьмой Всероссийской межотраслевой научно-технической конференции в рамках Второго Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во

СПбГМТУ, 2018, с. 78 – 86.
3. 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.
4. Алексеев А.В. Мониторинг и управление конкурентной способностью продукции как главный фактор технологического развития России / Перспективные направления развития отечественных информационных технологий: материалы IV межрегиональной научно-практической конф. Севастополь, 18-22 сентября 2018 г. / Севастопольский государственный университет; науч.ред. Б.В.Соколов. – Севастополь: СевГУ, 2018, с. 126-128.
5. Бобрович В.Ю., Антипов В.В., Смольников А.В., Алексеев А.В., Мусатенко Р.И. Ранговая партнерская сертификация качества и конкурентной способности объектов морской техники /Материалы 9-й конференции «Информационные технологии в управлении» (ИТУ-2016). - СПб.: АО «Концерн «ЦНИИ «Электроприбор», 2016, с. 263.
6. Алексеев А.В., Антипов В.А., Бобрович В.Ю., Евсеенко С.М. Реализация обобщенного метода квалиметрического анализа факторов развития и технология обеспечения управления развитием критических морских объектов // Морские интеллектуальные технологии. Научный журнал № 1 (31) Т.1, 2016, с. 27 – 37.
7. Алексеев А.В., Антипов В.В., Бобрович В.Ю., Смольников А.В. Развитие методологии ОМКАР и технологии обеспечения управления развитием критических морских объектов / 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, с. 428-429.
8. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В., Мусатенко Р.И. Прогнозирование успешности инновационных проектов развития из прошлого в будущее / Актуальные проблемы морской энергетики: материалы седьмой Всероссийской межотраслевой научно-технической конференции в рамках Второго Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2018, с. 411 – 415.
9. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В., Кузнецов В.В., Тычинин И.Ю. Конкурентная способность как главный фактор инвестиционной привлекательности / IV Санкт-Петербургский международный экономический конгресс (СПЭК-2018): материалы. – СПб.: НИИР им. С.Ю. Витте, 2018.04.2, с. 46 – 51.
10. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В., Бороненков И.М., Мусатенко Р.И. Автоматизация процессов борьбы за живучесть критических объектов: проблемы, лучшие практики, перспективы развития / XXI Всероссийская научно-практическая конференция «Актуальные проблемы защиты и безопасности», 3-6 апреля 2018: материалы. – СПб.: РАРАН, 2018, с. 57 – 62.
11. Александров В.Л., Алексеев А.В., Поляничко В.В., Ходан С.В. Организационно-технический мониторинг и управление приоритетным развитием индустриальной экономики «второго поколения» / IV Санкт-Петербургский международный экономический конгресс (СПЭК-2018): материалы. – СПб.: НИИР им. С.Ю.Витте, 2018.04.2, с. 16 – 21.
12. Жигадло В.Э. Основные задачи по реализации стратегии развития цифровой экономики в Санкт-Петербурге / Региональная информатика (РИ-2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Санкт-Петербург, 24-26 октября 2018 г.: Материалы конференции. \ СПОИСУ. – СПб, 2018, с. 63-64.
13. Программа «Цифровая экономика Российской Федерации», утвержденная распоряжением Правительства РФ 28 июля 2017 г. № 1632-р.
14. Орлов А.О. Цифровая путиномика / http://rusrand.ru/actuals/cifrovaya-putinomika.
15. Nicholas Negroponte — Bits & Atoms — University of Phoenix. Архивировано 16 октября 2013 года / https://ru.wikipedia.org/wiki/Электронная_экономика/
16. Что представляет собой цифровой переход? /http://impeltech.ru/blog/chto-predstavlyaet-soboy-cifrovoi-perehod/.
17. Белевцев А. Цифровизация — это фундаментальный тренд /http://www.up-pro.ru/library/strategy/tendencii/cyfra-trend.html/.
18. Революция в мозгах, или чем цифровизация отличается от автоматизации/http://www.up-pro.ru/library/strategy/tendencii/cyfra-avtomat.html.
19. Электронное правительство /https://ru.wikipedia.org/.
20. Алексеев А.В. Новая технология интеллектуальной поддержки мониторинга, прогнозирования и управления безопасностью объекта-района-города-региона / Перспективные направления развития отечественных информационных технологий: материалы III межрегиональной научно-практической конф. Севастополь, 19-23 сентября 2017 г. / Севастопольский государственный университет; науч.ред. Б.В.Соколов. – Севастополь: СевГУ, 2017, с. 44-46.
21. Алексеев А.В., Тычинин И.Ю., Мусатенко Р.И., Согонов С.А., Потехин В.С., Худобородов Е.Ф. Концепция роботизации управления как средства гарантированной поддержки качества функционирования критически важных объектов / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 5 \ СПОИСУ. – СПб, 2018, с. 442-446.

УДК 342.5

ГОСУДАРСТВЕННЫЕ УСЛУГИ НА ПУТИ К ЦИФРОВИЗАЦИИ

Дединкина Евгения Олеговна
Санкт-Петербургский информационно-аналитический центр
Черняховского ул., 59, Санкт-Петербург, 191040, Россия
e-mail: dedinkina@iac.spbu.ru

Аннотация. Рассмотрены понятия цифровой экономики. Определена значимость цифровой трансформации государственных услуг. Рассмотрена роль единой Межведомственной автоматизированной информационной системы предоставления в Санкт-Петербурге государственных и муниципальных услуг в электронном виде в развитии цифровой экономики региона. Представлены достигнутые положительные результаты Системы, сформулирована текущая проблематика.

Ключевые слова: электронные государственные услуги; цифровая экономика; электронное правительство.

PUBLIC SERVICES ON THE WAY TO DIGITALIZATION

Dedinkina Evgenia
St. Petersburg Information and Analytical Center
59 Chernyahovskogo Str., St. Petersburg, 191040, Russia
e-mail: dedinkina@iac.spbu.ru

Abstract. The article discusses the concepts of the digital economy and defines the significance of the public services digital transformation. The article describes the role of the Interagency computer information system of e-government service provision in St. Petersburg in the development of the regional digital economy. Also the article presents the current problems and the achieved positive results of the System functioning.

Keywords: e-government services; digital economy; e-government.

Введение.

«Цифровая экономика Российской Федерации» – это программа, утвержденная распоряжением Правительства Российской Федерации от 28.07.2017 № 1632-р (далее – Программа) [1], которая направлена на создание условий для улучшения благосостояния граждан путем повышения доступности и качества товаров и услуг с использованием современных цифровых технологий, повышения степени информированности и цифровой грамотности, улучшения доступности и качества государственных услуг. Ключевым фактором достижения целей Программы во всех сферах является перевод данных в цифровой формат.

Создание цифровой экономики – это масштабное предприятие, построенное на едином принципе оборота цифровых данных в таких областях, как образование и наука, социальное обеспечение, безопасность и другие – путем слияния в единую цифровую среду бизнеса, научно-образовательного сообщества, государства и граждан. Одним из ключевых направлений такого слияния является процесс оказания населению государственных услуг. В настоящее время во исполнение указа Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [2] в Санкт-Петербурге осуществляется подготовка региональной составляющей реализации Программы, в рамках которой особое значение приобретает курс на цифровую трансформацию государственных услуг. Осуществление цифровой трансформации государственных услуг в первую очередь предполагает реализацию процессов предоставления государственных услуг посредством современных IT-технологий в целях повышения качества, доступности и технологичности предоставления государственных услуг населению, минимизации административных барьеров, обеспечения необходимого уровня безопасности и защиты персональных данных, сокращения материальных и финансовых затрат, а также обеспечения максимального удобства для граждан и организаций в рамках процессов предоставления государственных услуг наряду с соблюдением принципов проактивности, экстерриториальности и многоканальности их предоставления.

Задача по обеспечению эффективной среды оказания государственных услуг населению с применением информационно-телекоммуникационных технологий не является новой. Более 10 лет назад в городе начала функционировать единая Межведомственная автоматизированная информационная система предоставления в Санкт-Петербурге государственных и муниципальных услуг в электронном виде (далее – МАИС ЭГУ, Система) [3]. Еще на этапе зарождения МАИС ЭГУ в процессы оказания услуг были заложены те принципы и задачи, которые сегодня отражает Программа. За годы работы МАИС ЭГУ достигла многомиллионного статуса, ведь число ее пользователей превышает 3 миллиона – граждане, представители бизнеса, исполнительные органы государственной власти Санкт-Петербурга (далее – ИОГВ) и пр.

МАИС ЭГУ состоит из множества различных компонентов, однако основная цель – обеспечение централизованного бизнес-процесса по оказанию услуг: прием заявлений, их регистрация, обработка, в том числе оборот сведений между ИОГВ и федеральными органами, принятие решения и выдача результата услуги. При этом следует отметить, что процесс является в действительности единым – вне зависимости от точки входа электронное заявление попадает в единую очередь. Портал «Государственные и муниципальные услуги (функции) в Санкт-Петербурге» (далее – Портал), где можно подать электронные заявления более чем по 200 услугам, мобильное приложение «Государственные услуги в Санкт-Петербурге», 57 стационарных и 4 мобильных многофункциональных центров (далее – МФЦ), 6 центров «Мой бизнес» – все это альтернативные возможные ресурсы для подачи заявлений в комфортной для заявителей форме. Кроме того, даже если заявитель подает заявление «традиционным» способом, то есть лично, его обработка и получение дополнительных сведений и документов, необходимых для оказания услуг, производится в цифровом формате.

Благодаря этому МАИС ЭГУ обеспечивает автоматизированный контроль соблюдения регламентированного порядка: сроки, документы, результаты – всю информацию заявители могут получить через Портал в онлайн-режиме. Контролирующие органы имеют оперативный доступ к соответствующим данным, поскольку все необходимые процессы и результаты представлены в электронной форме.

Ориентируясь на современные тенденции к созданию цифровой экономики, большая часть компонентов МАИС ЭГУ уже переведена на свободное программное обеспечение. Техническая реализация позволяет легко и удобно расширять возможности МАИС ЭГУ, интегрируя в нее новые функции, обеспечивая взаимодействие с другими государственными информационными системами. На данный момент обеспечено взаимодействие с 49 региональными, а также с 70 федеральными информационными системами органов власти. То есть единая взаимоинтегрированная цифровая среда ИОГВ в настоящее время уже построена.

Проведенные исследования показывают, что в 2018 году уровень удовлетворенности граждан качеством предоставления услуг составил 92,41%, а жители города осведомлены о преимуществах МФЦ и Портала, что говорит о достижении поставленных целей в значимой мере. Только в 2018 году по состоянию на 1 октября в городе подано более 39 миллионов электронных заявлений на получение государственных услуг, а по каналам межведомственного электронного взаимодействия передано более 87,4 миллионов запросов

сведений и документов. То есть именно столько раз заявителям не пришлось самостоятельно предоставлять дополнительную информацию в ИОГВ.

Также следует отметить, что МАИС ЭГУ получила призовые места в международных и всероссийских конкурсах, что говорит о ее эффективности в общепризнанном понимании, соответствии реализации Системы ожиданиям общества.

Основные достигнутые преимущества получения услуг в электронном виде для граждан заключаются в следующем: удобство подачи заявлений, где различные сведения уже заполнены автоматически, онлайн оплата пошлин, отсутствие очередей, сокращение количества взаимодействий с чиновником, онлайн-отслеживание статуса своего заявления – и даже получение результата услуги в электронном виде. На сегодняшний день удалось реализовать взаимодействие, при котором государственная услуга может предоставляться заявителю исключительно в электронном виде, а результат услуги, подписанный электронной подписью ответственного должностного лица, носит легитимный и правомерный характер.

В перспективе использование информационных технологий в процессе предоставления государственных услуг должно привести к полному отказу от бумажного эквивалента и необходимости предоставления заявителями документов на материальных носителях, а также привлечению в МАИС ЭГУ новых участников, в том числе коммерческих организаций, в частности – банков.

Говоря о трудностях, с которыми приходится сталкиваться в процессе перехода к цифровой экономике, следует отметить законодательные ограничения.

Сегодня во многом идентификация личности граждан требует визита заявителя в ИОГВ либо приобретения за свой счет сертификата электронной подписи [4], что исключает эффективную реализацию необходимого взаимодействия. Кроме этого, ряд актов, регулирующих порядок оказания услуг на федеральном уровне, предполагает личное участие заявителя в ряде процессов, например – представление оригиналов документов. Это пересекается с такой проблемой, как разница в уровне информатизации регионов России. К примеру, сегодня водитель такси обязан иметь «бумажную» лицензию для предъявления пассажиру по запросу [5]. Если же создать и нормативно закрепить электронный реестр лицензий, доступ к которому у граждан был бы обеспечен в режиме 24/7, владельцам такси бы не приходилось стоять в очередях за получением, переоформлением лицензий. Однако если в Санкт-Петербурге сегодня доступ к сети Интернет есть почти у каждого, то о соответствующей реализации в ряде других субъектов говорить несвоевременно. Решением проблемы послужит внесение изменений в ряд актов, допуская альтернативные решения в различных регионах страны.

Также проблематичным на сегодняшний день является тот факт, что несмотря на разработанную в МАИС ЭГУ возможность получения результатов услуг в виде электронных документов**,** являющихся абсолютной и легитимной альтернативой документов на бумажном носителе, владелец такого документа не сможет предъявить его во многих случаях – например, предъявить электронное удостоверение для получения скидки в частном музее. Ведь государственные структуры не охватывают всего масштаба жизнедеятельности и нужд граждан. В связи с этим необходимо повышение приоритета работ, направленных на взаимную интеграцию государства и коммерции, повышение уровня технической оснащенности на всех уровнях оказания гражданам государственных и негосударственных услуг и благ.

Что так же важно, на сегодняшний день ИОГВ продолжают осуществлять личное взаимодействие с заявителями по причине цифрового неравенства, отсутствия, к примеру, у лиц старшего поколения необходимых навыков работы с компьютером. Процесс оказания услуг должен оставаться доступным и понятным для всех категорий получателей услуг, будь то студенты или пенсионеры, родители или представители бизнес-сообщества. По этой причине большое значение уделяется популяризации возможностей МАИС ЭГУ среди населения и продвижению идеи развития информационного общества, повышения информационной грамотности граждан путем проведения мероприятий различных форматов – развлекательного, конкурсного, ознакомительного и обучающего характера. Также планируется реализация в Санкт-Петербурге программы, направленной на обучение широких масс населения использованию ресурсов информационного общества, в том числе электронного государства.

Заключение.

В целом можно заключить, что вся работа, направленная на дальнейшее развитие цифровой экономики в части предоставления государственных услуг, нацелена на комплексный эффект, начиная от увеличения количества и качества электронных услуг, сервисов и благ, заканчивая решением более высокоуровневых вопросов, что позволит централизованно прийти к высокой степени комфорта и доверия между обществом и государством и эффективной реализации цифровой экономики как в городе, так и в стране в целом. Реализуемые мероприятия позволят еще в большей мере достичь следующих результатов:

- повышение уровня осведомленности граждан о государственных услугах;
- повышение доступности и прозрачности процесса получения государственных услуг;
- повышение доверия граждан к государству, участие в процессах развития системы государственного управления;
- экономия времени и материальных затрат;
- сокращение и упразднение личного взаимодействия граждан с чиновниками.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении программы «Цифровая экономика Российской Федерации» [Электронный ресурс]: распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. Доступ из справ.-правовой системы «КонсультантПлюс».
2. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года [Электронный ресурс]: Указ Президента Российской Федерации от 7 мая 2018 года № 204 (ред. от 19 июля 2018 г.). Доступ из справ.-правовой системы «КонсультантПлюс».
3. О создании Межведомственной автоматизированной информационной системы предоставления в Санкт-Петербурге государственных и муниципальных услуг в электронном виде [Электронный ресурс]: постановление Правительства Санкт-Петербурга от 7 июня 2010 г. № 736 (ред. от 27 марта 2015 г.). Доступ из справ.-правовой системы «КонсультантПлюс».
4. О видах электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг [Электронный ресурс]: постановление Правительства Российской Федерации от 25 июня 2012 г. № 634 (ред. от 27 августа 2018 г.). Доступ из справ.-правовой системы «КонсультантПлюс».
5. Об утверждении правил перевозок пассажиров и багажа автомобильным транспортом и городским наземным электрическим транспортом [Электронный ресурс]: постановление Правительства Российской Федерации от 14 февраля 2009 г. № 112 (ред. от 28 апреля 2015 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

УДК621.396.2

ПРЕДЛОЖЕНИЯ ПО СОЗДАНИЮ ТИПОВОЙ ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ СВЯЗИ ОПОРНОЙ ЗОНЫ РАЗВИТИЯ В АРКТИКЕ

Кулешов Игорь Александрович, Солозобов Сергей Анатольевич, Шевченко Василий Васильевич
Информационные телекоммуникационные технологии
Кантемировская ул., 8, Санкт-Петербург, 197342, Россия
e-mail: Vasily.Shevchenko2014@yandex.ru

Аннотация. Рассмотрены положения Государственной Программы РФ «Социально-экономического развития Арктической зоны Российской Федерации» по формированию опорных зон развития в Арктике. Представлена типовая структура системы управления развития арктической опорной зоны. Разработана типовая территориально распределенная телекоммуникационная сеть связи опорной зоны развития в Арктике.

Ключевые слова: опорные зоны развития в Арктике**;** система управления**;** ситуационный центр**;** территориально распределенная телекоммуникационная сеть связи**;** типовой центр связи опорной зоны развития в Арктике.

PROPOSALS FOR THE CREATION OF THE MODEL OF THE GEOGRAPHICALLY DISTRIBUTED TELECOMMUNICATION NETWORK SUPPORT ZONE DEVELOPMENT IN THE ARCTIC

Kuleshov Igor, Solozobov Sergey, Shevchenko Vasily
Information and telecommunication technologies
8 Kantemirovskaya Str., St. Petersburg, 197342, Russia
e-mail: Vasily.Shevchenko2014@yandex.ru

Abstract. Provisions of the state Program of the Russian Federation «Social and economic development of the Arctic zone of the Russian Federation» on formation of basic zones of development in the Arctic are considered. The typical structure of the control system for the development of the Arctic reference zone is presented. A typical geographically distributed telecommunication network of the reference zone of development in the Arctic has been developed.

Keywords: reference zones of development in the Arctic**;** control system**;** situational center**;** geographically distributed telecommunication network**;** typical communication center of the reference zone of development in the Arctic.

Для дальнейшего освоения арктической зоны Российской Федерации Правительство РФ постановлением от 31 августа 2017 г. № 1064 внесло изменения в Государственную Программу РФ «Социально-экономического развития Арктической зоны Российской Федерации»[1].

Подпрограмма №1 этой программы называется «Формирование опорных зон развития и обеспечение их функционирования, создание условий для ускоренного социально - экономического развития Арктической зоны Российской Федерации». Новая редакция Программы развития Арктической зоны РФ разделила русское Заполярье на экономические опорные зоны. Территориальное деление было признано правительством более эффективным, чем отраслевое.

Исходя из существующего административно-территориального деления, функционирования транспортных узлов и ресурсной базы, а также перспектив социально-экономического развития Арктической зоны Российской Федерации и положений государственной программы «Социально-экономического развития Арктической зоны Российской Федерации» определены 8 опорных зон развития Арктической зоны Российской Федерации (Кольская, Архангельская, Ненецкая, Воркутинская, Ямало-Ненецкая, Таймыро-Туруханская, Северо-Якутская, Чукотская), что отображено на рис. 1.

Для каждой из них утвержден свой перечень приоритетных проектов, которые будут реализовываться на условиях государственно-частного партнерства. При грамотном использовании возможностей каждой зоны арктическая часть России может стать богатым и успешным промышленным макрорегионом.

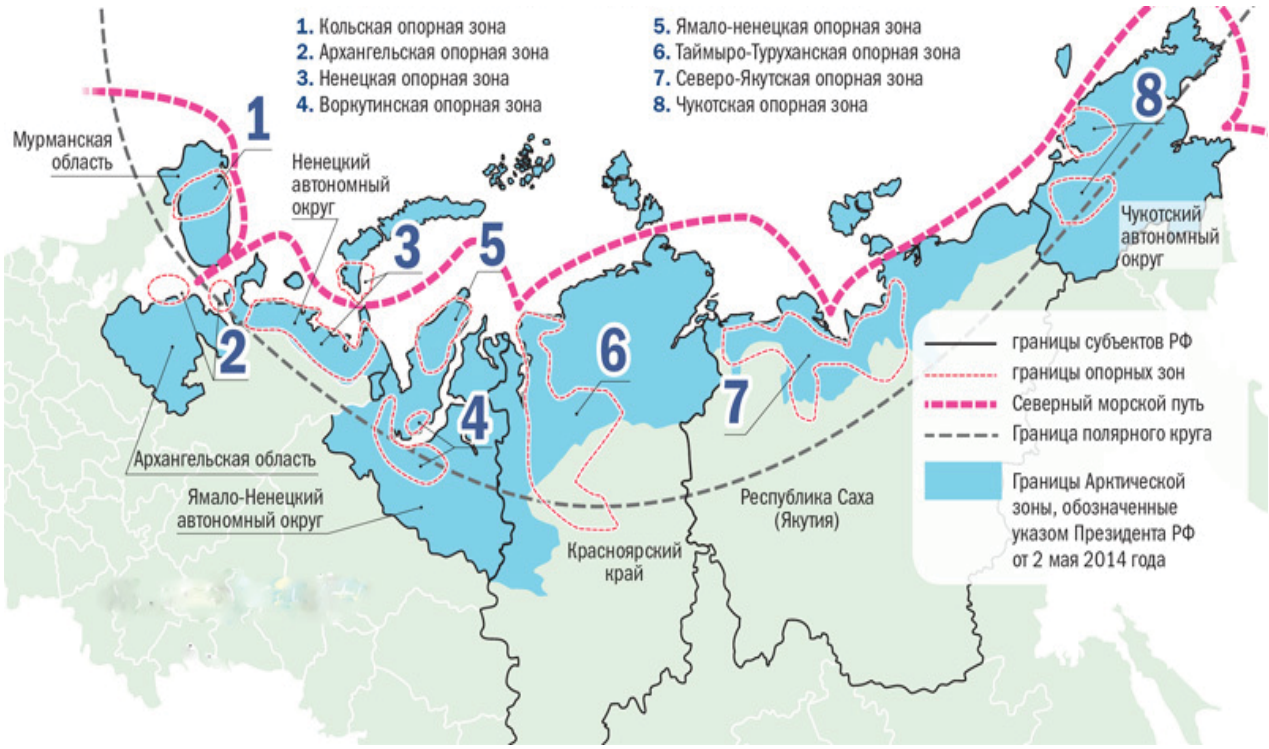


Рис. 1. Опорные зоны развития Арктического региона

Управление опорными зонами развития Арктического региона целесообразно осуществлять с ситуационных центров, расположенных в наиболее развитых с точки зрения инфраструктуры городах и населенных пунктах: Мурманск, Архангельск, Нарьян-Мар, Воркута, Сабетта, Норильск, Тикси, Певек. Главный ситуационный центр Арктической зоны предлагается разместить в Санкт-Петербурге.

Типовая структура системы управления в арктической опорной зоне развития включает:

1. Ситуационный центр пункта управления развитием опорной зоны.
2. Органы и пункты управления федерального уровня и местного самоуправления.
3. Органы и пункты управления частей и подразделений МО РФ, МЧС, ФСБ, МВД, Росгвардии.
4. Пункт управления (ПУ) Роскосмоса.
5. ПУ Министерства энергетики.
6. ПУ Министерства транспорта.
7. ПУ Росгидромета.
8. ПУ Росатома.
9. Пункты управления Министерства природных ресурсов и экологии.
10. Пункты управления Федеральной Службы по надзору в сфере природопользования.
11. ПУ различных Министерств и ведомств Российской Федерации, госкорпораций (с функцией сбора и передачи информации о состоянии на центры обработки данных).
12. Узлы связи, каналы и линии связи центра связи.
13. Центр обработки данных (с функцией предварительного анализа, визуализации информации состояния, принятия решения и формирование базы данных по опорной зоне).

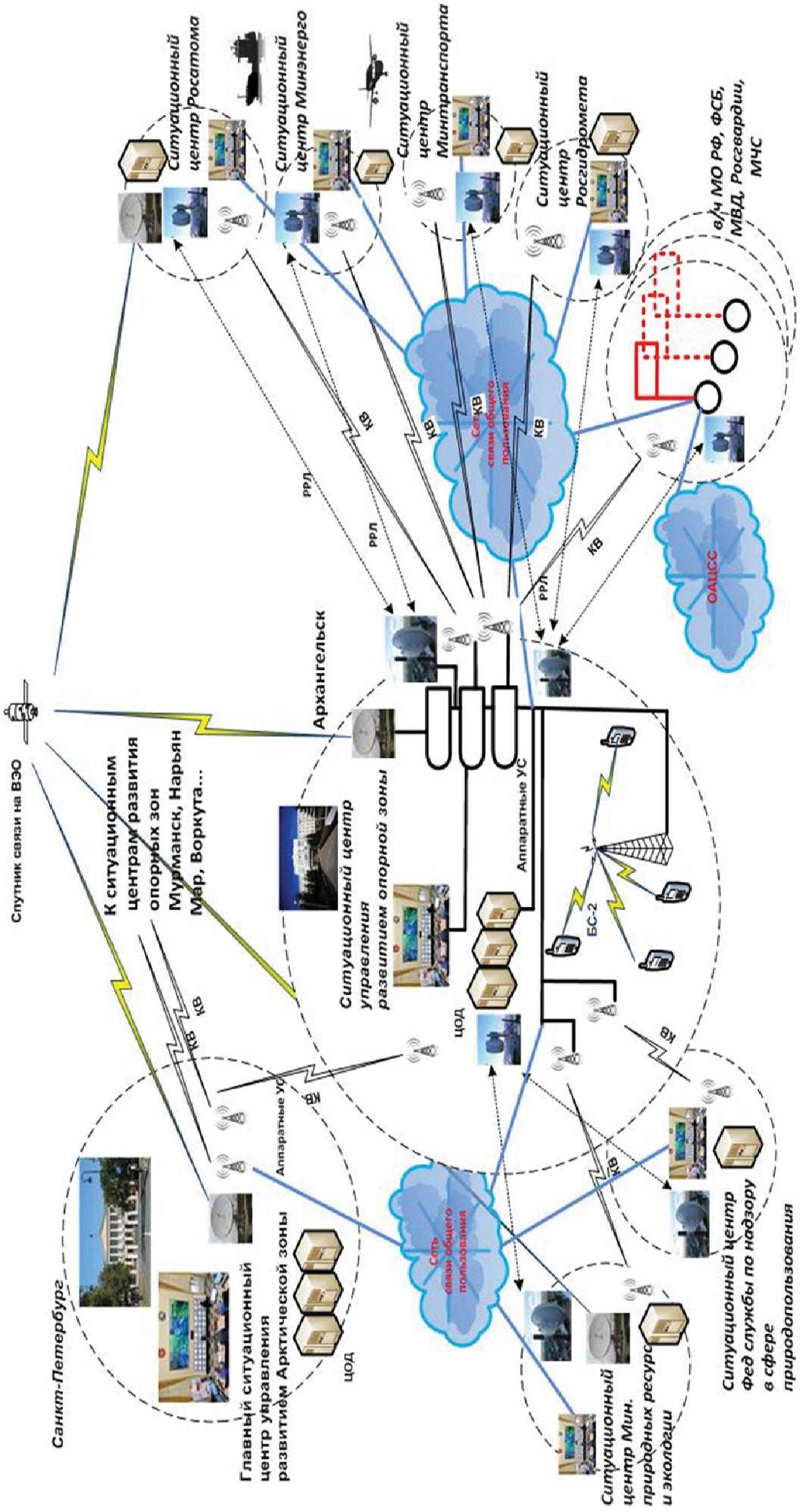
Связь от главного центра управления развитием Арктической зоны (Санкт-Петербург) с пунктами управления опорных зон развития (ПУ ОЗР) (Мурманск, Архангельск, Нарьян-Мар, Воркута, Сабетта, Норильск, Тикси, Певек) организуется следующим образом (рис. 2 Типовая территориально распределенная телекоммуникационная система связи опорной зоны развития в Арктике):

– спутниковая связь через космические аппараты связи «Меридиан» (а в перспективе – через космическую систему «Арктика МС») на высоко-элиптической орбите или спутниковую систему связи – «Гонец – Д1М» на низкой - (1400 км) орбите;

– спутниковая связь на инстанцию ниже организуется с наиболее важными ПУ РОЗ – ПУ Росатома, Министерства природных ресурсов и экологии и др.;

– КВ радиосвязь ионосферной волной возможна с ПУ РОЗ на расстояние до 2 - 3 тыс. км. (Мурманск, Архангельск, Нарьян-Мар, Воркута).

В перспективе при создании в Арктике КВ радиосети и обеспечения устойчивой радиосвязи для опорных зон развития, необходимо будет создавать радиоретрансляционные центры. Потребуется 3 - 4 центра.


Спутник связи на ВЭО
К ситуационным центрам развития опорных зон Мурманск, Нарьян Мар, Воркута...
Ситуационный центр Росатома
Ситуационный центр Минэнерго
Ситуационный центр Минтранспорта
Ситуационный центр Росгидромета
в/ч МО РФ, ФСБ, МВД, Росгвардии, МЧС
Архангельск
Ситуационный центр управления развитием опорной зоны
Аппаратные УС
ЦОД
БС-2
РРЛ
КВ
Сеть связи общего пользования
ОАЦСС
Санкт-Петербург
Главный ситуационный центр управления развитием Арктической зоны
Ситуационный центр Мин. природных ресурсов и экологии
Ситуационный центр Фед службы по надзору в сфере природопользования

Они позволят обеспечить меридианные направления радиосвязи относительно устойчивые от ионосферных возмущений, вызванных полярными сияниями.

Предлагается использовать существующие радиоцентры в Подмосковье – в Ногинске, Екатеринбурге, Омске, Красноярске и Якутске. Радиотрассы, организованные от этих центров, будут односкачковыми и иметь протяженность 2200 – 2600 км. Телефонная связь и передача данных организуются через сеть связи общего пользования (ССОП), созданную Ростелекомом и другими операторами связи.

Связь от пункта управления развитием Арктической зоны с пунктами управления различных министерств и ведомств в пределах опорной зоны развития организуется следующим образом:

– спутниковая связь - через спутники связи типа «Меридиан» на высокоэлиптической орбите или спутниковую систему связи – «Гонец – Д1М» на низкой орбите с наиболее важными пунктами управления РОЗ пунктами управления Росатома, Министерства природных ресурсов и экологии и др.

В качестве оконечных станций спутниковой связи предлагается использовать Р-441, Р-444-ПТН и Р-444-ПТД:

– радиорелейная связь с основными пунктами управления внутри опорной зоны развития с помощью специальных мобильных комплексов СМК-О;

– с дальностью связи до 30 км или Р-431.- КВ радиосвязь с ПУ РОЗ земной волной – до 40 км или ионосферной волной на расстояние до 2 тыс. км.

Телефонная связь и передача данных с ПУ министерств и ведомств организуется через сети связи общего пользования (ССОП).

В перспективе необходимо связать все опорные зоны тропосферными средствами связи на новых ТРС с дальностью действия до 500 км. Для связи вдоль всего побережья Северного Ледовитого океана и на основных островах потребуется 28÷30 тропосферных станций [2].

На объектах организуется радиодоступ и УКВ радиосвязь с помощью абонентских носимых станций. Радиодоступ возможен с помощью базовых станций (БС) «Мир» на дальность до 40 км, номерной емкостью более 1300 абонентов.

Каждый ситуационный центр опорной зоны развития включает в свой состав центр обработки данных. В ЦОД осуществляются обработка любой информации, то есть создание или генерирование данных, последующее архивирование и хранение файлов, а также предоставление их по запросу пользователей. ЦОДы являются распределенными.

Для обеспечения устойчивой работы пользователей между элементами распределенного ЦОД организуются отказоустойчивые каналы связи.

На сегодняшний день почти в каждом регионе уже присутствуют несколько операторов магистральной передачи данных, услуги которых можно использовать [3].

Предлагается следующий состав типового центра связи опорной зоны развития в Арктике (см. Табл. 1):

Таблица 1

Тип средства связи	Количество
ЦРПУ «Москвичка-ПРМ»	1
МРПУ УКВ	2
Многотрактовые передатчики КВ, мощностью 1 и 5 кВт	2-3
УКВ радиостанции Р-620	8
Радиорелейные станции Р-431	2-3
Радиорелейные станции СМК-О	2
Станции спутниковой связи Р-441	3-4
БС «Мир»	По количеству ПУ в ОЗР

Заключение.

Предложенная типовая территориально распределенная телекоммуникационная сеть связи опорной зоны развития в Арктике позволит обеспечить устойчивое управление из ситуационных центров.

СПИСОК ЛИТЕРАТУРЫ

1. Государственная Программа Российской Федерации «Социально-экономическое развитие Арктической зоны Российской Федерации» (в редакции постановления Правительства Российской Федерации от 31 августа 2017 г. № 1064).
2. Предложения по построению сети тропосферной радиосвязи в Арктике / И.А. Кулешов, С.А. Солозобов, Ю.Ф. Махортов, В.В. Шевченко // Сборник тезисов на IV Всероссийской научно - техн. конф. «Системы связи и радионавигации», г. Красноярск, 12-13 нояб. 2017.- С. 12-19.
3. Савин Н. Что необходимо для построения распределенного ЦОД?// Connect! № 8, август, 2006.

УДК 004.056

ОСНОВНЫЕ НАПРАВЛЕНИЯ РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Сторожик Виктор Сергеевич
Управление ФСТЭК России по Северо-Западному федеральному округу
Исаакиевская пл., 11, Санкт-Петербург, 190000, Россия
e-mail: szfo@fstec.ru

Аннотация. Рассматриваются нормативные правовые акты и методические документы, определяющие основные направления реализации государственной политики в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, а также предусмотренные ими первоочередные меры в части категорирования объектов критической информационной инфраструктуры, методического обеспечения защиты информационных и автоматизированных систем объектов критической информационной инфраструктуры и содержащейся в них информации, разъяснения правил осуществления ФСТЭК России и ее территориальными органами мероприятий по государственному контролю значимых объектов критической информационной инфраструктуры.

Ключевые слова: автоматизированная система управления; безопасность критической информационной инфраструктуры; государственный контроль; значимый объект критической информационной инфраструктуры; информационная система; информационно-телекоммуникационная сеть; категории значимости; компьютерная атака; компьютерный инцидент; критическая информационная инфраструктура; объект критической информационной инфраструктуры; показатель критерия значимости; субъект критической информационной инфраструктуры; угрозы безопасности информации.

THE MAIN DIRECTIONS OF THE STATE POLICY IN THE FIELD OF SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

Storozhik Victor
The office of the FSTEC of Russia in the Northwest Federal district
11 Isaakievskaya Sq., St. Petersburg, 190000, Russia
e-mail: szfo@fstec.ru

Abstract. The normative legal acts and methodical documents defining the main directions of implementation of the state policy in the field of safety of critical information infrastructure of the Russian Federation, and also the priority measures provided by them regarding categorization of objects of critical information infrastructure, methodical ensuring protection of information and automated systems of objects of critical information infrastructure and the information containing in them are considered, clarification of the rules of implementation of the FSTEC of Russia and its territorial bodies of measures for state control of significant objects of critical information infrastructure.

Keywords: automated control system; security of critical information infrastructure; state control; significant object of critical information infrastructure; information system; information and telecommunication network; significance categories; computer attack; computer incident; critical information infrastructure; object of critical information infrastructure; significance criterion indicator; subject of critical information infrastructure; information security threats.

Введение.

В Концепции внешней политики Российской Федерации, утвержденной Указом Президента Российской Федерации от 30 ноября 2016 г. № 640 сформулирована позиция государства по отношению к использованию информационно-коммуникационных технологий в современном мире. В документе отмечено, что Российская Федерация принимает необходимые меры для обеспечения национальной и международной информационной безопасности, и противодействия угрозам государственной, экономической и общественной безопасности, исходящим из информационного пространства.

В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 определены стратегические цели и основные направления обеспечения информационной безопасности государства с учетом его стратегических национальных приоритетов. При этом к основным национальным интересам в информационной сфере отнесено обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (КИИ) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время.

Ярким примером деструктивного воздействия злоумышленников на КИИ являются масштабные компьютерные инциденты в мае - июне 2017 года, вызванные распространением вредоносного программного обеспечения типа WannaCry, Petya, Misha и их модификаций, в результате которых было нарушено штатное функционирование информационных систем некоторых федеральных органов исполнительной власти, а также ряда объектов, которые относятся к КИИ (АО «РЖД», Сбербанк России, Пенсионный фонд Российской

Федерации, ОАО «Мегафон» и другие). Устранение последствий данных деструктивных воздействий в ряде случаев потребовало серьезных усилий специалистов в области информационной безопасности.

Определяющую роль в решении задач повышения уровня защищенности информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, функционирующих в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а так же российских юридических лиц и (или) индивидуальных предпринимателей, которые обеспечивают взаимодействие указанных систем или сетей, играет Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который вступил в силу с 1 января 2018 г. В данном федеральном законе определены: организационные и правовые основы обеспечения безопасности КИИ, а также основные принципы обеспечения безопасности КИИ; полномочия государственных органов в этой области; права, обязанности и ответственность лиц, владеющих на праве собственности или другом законном основании объектами КИИ, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов.

К принципам обеспечения безопасности КИИ федеральным законом отнесены: законность; непрерывность и комплексность обеспечения безопасности КИИ достигаемые, в том числе, за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов КИИ; приоритет предотвращения компьютерных атак.

В целях реализации норм данного федерального закона Указом Президента Российской Федерации от 25 ноября 2017 г. № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085» ФСТЭК России определена как федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, а Указом Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» ФСБ России определена как федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

В соответствии с Планом-графиком подготовки нормативных правовых актов Российской Федерации, Правительства Российской Федерации и федеральных органов исполнительной власти, необходимых для реализации норм Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», утвержденным Заместителем Председателя Правительства Российской Федерации от 28 августа 2017 г. № 5985п-П10 разработана система нормативных правовых актов и методических документов Правительства Российской Федерации и федеральных органов исполнительной власти (ФСТЭК России, ФСБ России и Минкомсвязи России), определяющих порядок реализации основных направлений государственной политики в области обеспечения безопасности КИИ, в том числе организацию межведомственной координации и взаимодействия, специальные и контрольные функции Федеральной службы по техническому и экспортному контролю.

Нормативные правовые акты в области обеспечения безопасности КИИ, разработанные Правительством Российской Федерации:

1. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

2. Постановление Правительства Российской Федерации от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры».

Правительством Российской Федерации также подготовлен проект постановления «Об утверждении порядка подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры».

Нормативные правовые акты в области обеспечения безопасности КИИ, разработанные ФСТЭК России:

1. Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов КИИ» (зарегистрирован в Минюсте России 22 февраля 2018 г. № 50118).

2. Приказ ФСТЭК России от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости» (зарегистрирован в Минюсте России 13 апреля 2018 г. № 50753).

3. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ» (зарегистрирован в Минюсте России 26 марта 2018 г. № 50524).

4. Приказ ФСТЭК России от 11 декабря 2017 г. № 229 «Об утверждении формы акта проверки» (зарегистрирован в Минюсте России 28 декабря 2017 г. № 49500).

5. Приказ ФСТЭК России от 6 декабря 2017 г. № 227 «Об утверждении порядка ведения реестра значимых объектов КИИ» зарегистрирован в Минюсте России 8 февраля 2018 г. № 49966).

6. Приказ ФСТЭК России от 09 августа 2018 г. № 138 «О внесении изменений в Требования 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, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239» (зарегистрирован в Минюсте России 5 сентября 2018 г. № 52071).

Нормативные правовые акты в области обеспечения безопасности КИИ, разработанные ФСБ России:

1. Приказ ФСБ России от 27 августа 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» (зарегистрирован в Минюсте России 6 сентября 2018 г. № 52109).

2. Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка ее представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (зарегистрирован в Минюсте России 6 сентября 2018 г. № 52108).

3. Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» (зарегистрирован в Минюсте России 6 сентября 2018 г. № 52107).

Минкомсвязи России осуществляет работу над проектом приказа «Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак на сетях связи».

При разработке нормативных правовых актов ФСТЭК России по обеспечению безопасности КИИ были учтены положения и опыт реализации:

– «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119;

– «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17;

– «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных приказом ФСТЭК России от 18 февраля 2013 г. № 21;

– «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», утвержденных приказом ФСТЭК России от 14 марта 2014 г. № 31.

К обсуждению проектов нормативных правовых актов ФСТЭК России по обеспечению безопасности КИИ были привлечены представители более 40 крупнейших субъектов КИИ.

В качестве первоочередных практических мер по обеспечению безопасности объектов КИИ нормативными правовыми актах предусмотрены:

– категорирование объектов КИИ;
– создание систем безопасности значимых объектов КИИ;
– реализация требований по обеспечению безопасности значимых объектов КИИ;
– обеспечение взаимодействия значимых объектов КИИ с ГосСОПКА.

Постановлением Правительства Российской Федерации от 8 февраля 2018 г. №127 утверждены правила категорирования объектов КИИ, а также перечень показателей критериев значимости объектов КИИ и их значения. Показатели разработаны с учетом нормативных правовых актов, регулирующих правоотношения в сфере связи, топливно-энергетическом комплексе, использования атомной энергии, транспортной безопасности, безопасности гидротехнических сооружений, промышленной безопасности, с учетом предложений уполномоченных федеральных органов исполнительной власти и значительного числа наиболее важных субъектов КИИ.

При этом категорирование объектов КИИ представляет собой процесс отнесения объектов критической информационной инфраструктуры к одной из трех установленных категорий или определение отсутствия необходимости присвоения какой-либо категории посредством априорной оценки значений показателей критериев значимости из утвержденного перечня.

В качестве субъектов КИИ в процессе категорирования рассматриваются: государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым принадлежат объекты КИИ, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления или сетей (операторы связи). Если субъект КИИ принимает решение, что он не является таковым и не должен проводить категорирование, то федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ (ФСТЭК России), обладает возможностью направить субъекту КИИ требование о необходимости представления сведений о результатах категорирования либо об отсутствии категории.

В качестве объектов КИИ в процессе категорирования рассматриваются: информационные системы, информационно-телекоммуникационных сети, автоматизированные системы управления, принадлежащие субъекту КИИ на праве собственности, аренды или ином законном основании. В статье 209 Гражданского кодекса Российской Федерации «Содержание права собственности» указывается, что основание – это документ, в котором определено, что пользователь получил от владельца объекта право на его использование в течении определенного периода на условиях, установленных собственником (договор пользования, договор на право хозяйственного ведения, договор на право оперативного управления и т.п.).

Для проведения категорирования решением руководителя субъекта КИИ создается Комиссия по категорированию, которую возглавляет руководитель субъекта КИИ или уполномоченное им лицо. В комиссию входят: работники субъекта КИИ, являющиеся специалистами в области выполняемых функций, осуществляемых видов деятельности, в области информационных технологий и связи, по эксплуатации основного технологического оборудования, работники субъекта КИИ, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов КИИ; работники субъекта КИИ, на которых возложены функции обеспечения безопасности объектов КИИ; работники субъекта КИИ, на которых возложены функции обеспечения безопасности объектов КИИ; работники структурного подразделения по ГО и ЧС или работники, уполномоченные на решение задач в этой области. В состав могут включаться представители государственных органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности (ЦБ РФ (Банк России), ГК «Росатом» и ГК «Роскосмос»), по согласованию с ними.

Мероприятия, проводимые комиссией по категорированию объектов КИИ, включают:

– определение управленческих, технологических, производственных, финансово – экономических и иные процессов, обеспечиваемых в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ;

– выявление наличия критических процессов у субъекта КИИ;

– выявление объектов КИИ, которые обрабатывают информацию, необходимую для выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

– подготовка предложений для включения в перечень объектов КИИ подлежащих категорированию;

– рассмотрение возможных действий нарушителей в отношении объектов КИИ, а также иных источников угроз безопасности информации (УБИ);

– анализ УБИ и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ;

– оценку масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ;

– установление каждому из объектов КИИ одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им категорий значимости.

Исходные данные для категорирования объекта КИИ включают:

– сведения об объекте КИИ: назначение, архитектура объекта, применяемые программные и аппаратно-программные средства, взаимодействие с другими объектами КИИ, наличие и характеристики доступа к сетям связи;

– процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ;

– состав информации, обрабатываемой объектами КИИ, сервисы по управлению, контролю или мониторингу, предоставляемые объектами КИИ;

– декларацию промышленной безопасности опасного производственного объекта, декларацию безопасности гидротехнического сооружения, паспорт объекта топливно-энергетического комплекса, на которых функционирует объект КИИ, если их разработка предусмотрена законодательством Российской Федерации;

– сведения о взаимодействии объекта КИИ с другими объектами КИИ и (или) зависимость от их функционирования;

– модели угроз безопасности информации и нарушителей в отношении объекта КИИ, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах КИИ данного типа.

При этом в соответствии с информационным сообщением ФСТЭК России от 4 мая 2018 г. № 240/22/2339 «О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации» до утверждения в установленном порядке

«Методики определения угроз безопасности информации в информационных системах Российской Федерации» необходимо руководствоваться при моделировании угроз безопасности информации на объектах КИИ:

– «Базовой моделью угроз безопасности информации в ключевых системах информационной инфраструктуры», утвержденной ФСТЭК России 18 мая 2007 г.;

– «Методикой определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры», утвержденной ФСТЭК России 18 мая 2007 г.;

– «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной ФСТЭК России 15 февраля 2008 г.;

– «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной ФСТЭК России 14 февраля 2008 г.

В процессе категорирования детализация объекта КИИ определяется на основании эксплуатационной и технической документации объекта КИИ и с учетом обеспечиваемых критических процессов.

Объединение в один объект нескольких объектов КИИ возможно, если эти объекты взаимосвязаны или обеспечивают хотя бы один общий критический процесс.

Оценка масштаба возможных последствий в случае возникновения компьютерных инцидентов должна определяться как результат нарушения функционирования единого (объединенного) объекта КИИ, а не отдельных его узлов.

Перечень объектов КИИ подлежащих категорированию необходимо оформлять по форме рекомендованной Информационным сообщением ФСТЭК России от 24 августа 2018 г. № 240/25/3752. Перечень подлежит согласованию с государственным органом или российским юридическим лицом, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере в части подведомственных им субъектов КИИ, утверждается руководителем субъекта КИИ и в течение 5 дней после утверждения подлежит представлению в ФСТЭК России.

Максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом критической информационной инфраструктуры перечня объектов.

Решение комиссии по категорированию оформляется актом, который должен содержать: сведения об объекте КИИ; результаты анализа угроз безопасности информации объекта КИИ; реализованные меры по обеспечению безопасности объекта КИИ; сведения о присвоенной объекту КИИ категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, установленными ФСТЭК России.

Категорирование объектов КИИ включает:

– определение всех процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ;

– выявление процессов, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка, выраженным в показателях критериев значимости (критические процессы);

– определение объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, формирование перечня объектов КИИ, подлежащих категорированию;

– оценку в соответствии со значениями показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ;

– установление соответствия объектов КИИ значениям показателей критериев значимости и присвоение каждому из них одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

Оценка возможного ущерба формируется на основании анализа возможных рисков в процессе качественного описания сценариев развития неблагоприятных ситуаций, оценки вероятности их возникновения и характеризует негативный результат воздействия.

Масштаб возможных последствий отражает степень значения или влияния на окружающую действительность негативного результата воздействия.

Значимость отражает степень важности, измерение, разработанное в попытках получить объективную характеристику процессов в различных сферах деятельности: социальной; политической; экономической; экологической; обороны, безопасности и правопорядка.

Оценка производится по каждому из значений показателей критериев значимости, а категория присваивается по наивысшему значению.

В соответствии с указаниями Информационного сообщения ФСТЭК России от 24 августа 2018 г. № 240/25/3752 предоставление информации об отсутствии в организации объектов КИИ или о том, что организация не является субъектом КИИ Российской Федерации в ФСТЭК России в соответствии с законодательством о безопасности критической информационной инфраструктуры Российской Федерации не требуется.

Приказом ФСТЭК России от 22 декабря 2017 г. № 236 утверждена форма направления сведений о результатах присвоения объекту КИИ Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, которая должна содержать:

– сведения об объекте КИИ (наименование, места (адреса) размещения, сфера (область) деятельности, назначение и критические процессы, для обеспечения которых используется объект критической информационной инфраструктуры, архитектура этого объекта);

– сведения о субъекте КИИ, которому на праве собственности, аренды или ином законном основании принадлежит объект КИИ (наименование, юридический и фактический адреса, подразделение (работники), на которое (которых) возложены функции по обеспечению безопасности объекта КИИ);

– сведения о взаимодействии объекта КИИ и сетей электросвязи с указанием наименования сетей электросвязи и способов взаимодействия;

– сведения о лице, эксплуатирующем объект КИИ (наименование, юридический и фактический адреса);

– сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ, в том числе средствах, используемых для обеспечения безопасности объекта КИИ и их сертификатах соответствия требованиям по безопасности информации (при наличии);

– сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ либо об отсутствии таких угроз;

– возможные последствия в случае возникновения компьютерных инцидентов на объекте КИИ либо сведения об отсутствии таких последствий;

– категория значимости, которая присвоена объекту КИИ, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости;

– организационные и технические меры, применяемые для обеспечения безопасности объекта КИИ, либо сведения об отсутствии необходимости применения указанных мер.

ФСТЭК России в целях приведения в соответствие мер по 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 и мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации издан приказ от 9 августа 2018 г. № 138 «О внесении изменений в Требования 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, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239», который прошел независимую антикоррупционную экспертизу и общественное обсуждение. Ведется подготовка проекта методического документа ФСТЭК России «Меры защиты информационных и автоматизированных систем и содержащейся в них информации», в котором конкретизируется подход к выбору мер защиты информации, а также производится детализация мер обеспечения безопасности принимаемых на значимых объектах критической информационной инфраструктуры Российской Федерации.

Постановлением Правительства Российской Федерации от 17 февраля 2018 г. № 162 определены правила осуществления ФСТЭК России и ее территориальными органами мероприятий по государственному контролю в области обеспечения безопасности значимых объектов КИИ РФ. При этом предусмотрено проведение двух видов государственного контроля: плановая и внеплановая проверки.

Основания для осуществления плановой проверки определяются исходя из следующих условий:

– истечение 3 лет со дня внесения сведений об объекте КИИ в реестр значимых объектов КИИ;

– окончание осуществления последней плановой проверки в отношении значимого объекта КИИ.

– Основания для осуществления внеплановой проверки определяются исходя из следующих условий:

– истечение срока выполнения субъектом КИИ выданного органом государственного контроля предписания об устранении выявленного нарушения требований по обеспечению безопасности;

– возникновение компьютерного инцидента на значимом объекте КИИ, повлекшего негативные последствия;

– поручение Президента Российской Федерации или Правительства Российской Федерации;

– требование прокурора в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

Заключение.

Таким образом, рассмотрена система нормативных правовых актов Правительства Российской Федерации, ФСТЭК России, ФСБ России и Минкомсвязи России, определяющих порядок реализации основных направлений государственной политики в области обеспечения безопасности КИИ, в том числе организацию межведомственной координации и взаимодействия, специальные и контрольные функции Федеральной службы по техническому и экспортному контролю. Особое внимание уделено первоочередным практическим мерам по обеспечению безопасности объектов КИИ, которые предусмотрены нормативными правовыми актами

Правительства Российской Федерации и ФСТЭК России, в части категорирования объектов КИИ, методического обеспечения защиты информационных и автоматизированных систем объектов КИИ и содержащейся в них информации, разъяснения правил осуществления ФСТЭК России и ее территориальными органами мероприятий по государственному контролю значимых объектов КИИ.

СПИСОК ЛИТЕРАТУРЫ

1. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 31 декабря 2015 г. № 683).
2. Концепция внешней политики Российской Федерации (утв. Указом Президента Российской Федерации от 30 ноября 2016 г. № 640).
3. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).
4. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ (ред. от 3 августа 2018 г.) (с изм. и доп., вступ. в силу с1 сентября 2018 г.).
5. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
6. Указ Президента Российской Федерации от 25 ноября 2017 г. № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085».
7. Указ Президента Российской Федерации от 2 марта 2018 г. № 98 «О внесении изменений в Перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента РФ от 30 ноября 1995 г. № 1203».
8. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
9. Постановление Правительства Российской Федерации от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры».
10. Проект постановления Правительства Российской Федерации «Об утверждении порядка подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов КИИ».
11. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
12. Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов КИИ» (зарегистрирован в Минюсте России 22 февраля 2018 г. № 50118).
13. Приказ ФСТЭК России от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости» (зарегистрирован в Минюсте России 13 апреля 2018 г. № 50753).
14. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ» (зарегистрирован в Минюсте России 26 марта 2018 г. № 50524).
15. Приказ ФСТЭК России от 11 декабря 2017 г. № 229 «Об утверждении формы акта проверки» (зарегистрирован в Минюсте России 28 декабря 2017 г. № 49500).
16. Приказ ФСТЭК России от 6 декабря 2017 г. № 227 «Об утверждении порядка ведения реестра значимых объектов КИИ» зарегистрирован в Минюсте России 8 февраля 2018 г. № 49966).
17. Приказ ФСТЭК России от 9 августа 2018 г. № 138 «О внесении изменений в Требования 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, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239» (зарегистрирован в Минюсте России 05 сентября 2018 г. № 52071).
18. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
19. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
20. 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».
21. Приказ ФСБ России от 27 августа 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» (зарегистрирован в Минюсте России 6 сентября 2018 г. № 52109).
22. Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка ее представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (зарегистрирован в Минюсте России 6 сентября 2018 г. № 52108).
23. Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» (зарегистрирован в Минюсте России 6 сентября 2018 г. № 52107).
24. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утверждена ФСТЭК России 18 мая 2007 г.
25. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, утверждена ФСТЭК России 18 мая 2007 г.
26. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена ФСТЭК России 15 февраля 2008 г.
27. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена ФСТЭК России 14 февраля 2008 г.

УДК 004.03, 004.05, 004.6, 004.7

ВОПРОСЫ ИНТЕРОПЕРАБЕЛЬНОСТИ ГОРОДСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ САНКТ-ПЕТЕРБУРГА

Шиян Артём Викторович, Митягин Сергей Александрович
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)
Биржевая линия 14, Санкт-Петербург, 199034, Россия
e-mails: artem.shiyan68@gmail.com, mityagin.spb@gmail.com

Аннотация. В статье рассматривается исследование механизмов интероперабельности в масштабе ИТ-инфраструктуры города, представленной множеством взаимодействующих информационных систем, а также формат анализа уровня схожести информационных систем для практических рекомендаций по реструктуризации существующего шаблона проектирования систем и реорганизации их взаимодействия. Для этого проводится многоэтапное исследование систем разных функциональных уровней. По результатам анализа предложены рекомендации по развитию городской ИТ-инфраструктуры.

Ключевые слова: интероперабельность; информационная инфраструктура; информационная система; умный город.

ISSUES OF URBAN INFORMATION SYSTEMS INTEROPERABILITY in ST. PETERSBURG

Shiyan Artem, Mityagin Sergey
The St. Petersburg National Research University of Information Technologies, Mechanics and Optics (University ITMO)
14 Birzhevaya Linia, St. Petersburg, 199034, Russia
e-mails: artem.shiyan68@gmail.com, mityagin.spb@gmail.com

Abstract. The paper examines the study of interoperability mechanisms in the scale of urban IT infrastructure, represented by a variety of interacting information systems and also framework analysis of the similarity level about information systems for practical recommendations on restructuring the existing design pattern of systems and reorganization of their interaction. And it is also include the advanced multi-stage study about different functional levels. Based on these systems interoperability research, recommendations for the development of urban IT infrastructure are given.

Keywords: interoperability; information infrastructure; information system; smart city.

Введение. Обозначая ИТ-инфраструктуру как критический элемент влияния на городские процессы, важно знать, насколько функциональность, целостность, структура и параметры качества обработки данных существующих информационных систем соответствуют текущим целям развития города, приоритетным задачам городского планирования, новым вызовам при проектировании экосистемы умного города [1].

Государственные информационные системы, согласно существующему законодательству, автоматизируют исключительно определенный перечень приоритетных функциональных услуг, что приводит к недостаточной гибкости структуры обмена данными. Кроме этого, являясь ключевыми элементами межведомственных процессов взаимодействия они влияют на формирование каркаса единого информационного пространства. Исторически сохранившиеся системообразующие параметры разрозненности отдельных элементов городской инфраструктуры обуславливают рост типовых проблем способности систем к взаимодействию между собой. Окончательное урегулирование данного вопроса может быть обеспечено за счет изменения требований к технологиям и регламенту взаимодействия: реструктуризацией существующих государственных информационных систем, реорганизацией шаблона проектирования и изменением фундаментальных принципов конфигурации городской ИТ-инфраструктуры [2].

На сегодняшний день в совокупности Санкт-Петербург имеет оперативно-стратегический инфраструктурный комплекс из более чем 200 ежедневно функционирующих систем.

Формат классификации объектов городского комплекса информатизации приведен в Таблице 1.

Таблица 1

Распределение систем по статусу в городском информационном пространстве

Категория	**Детализированные сведения**	
	Общее кол-во	**Примеры перечисленных систем**
Ключевой узел	3	РСМЭВ, МАИС ЭГУ, УЦ ИОГВ
Системообразующий узел	2	ТОРИС и КАИС КРО
Большой узел	10	АПК БГ, ГИППС, ГАС ФН ПДД
Стандартный узел	201	первичные элементы сети

Актуальная структура межведомственной сети городского взаимодействия разделена на четыре уровня. Основными элементами являются городские информационные системы. На следующем уровне - системы

федерального значения (интеграция в информационное пространство высших государственных структур). Не менее важный статус имеют региональные информационные системы, которые зачастую дополняют функционал городских информационных систем. А в качестве последних элементов конфигурации выступают общедоступные системы (порталы и открытые данные). На рис. 1 представлен каркас ИТ-инфраструктуры согласно наборам городских данных [3].

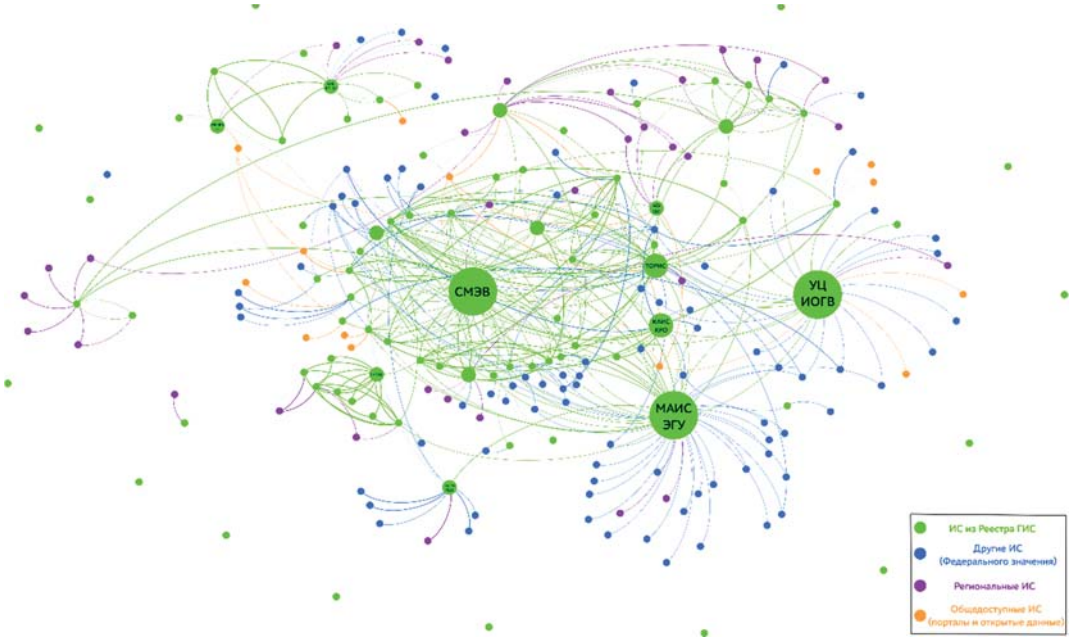


Рис. 1. Визуализация связей между информационными системами Санкт-Петербурга

В рамках логики интеграционных процессов предложена структурно-функциональная модель умного города. Такая платформа представляет собой взаимосвязанный набор функциональных элементов инфраструктуры цифровой экономики города, и базируется на четырех слоях [4, 5].

Слой физических средств информационного взаимодействия - обеспечивает бесшовную интеграцию первичных инфраструктурных цифровых элементов в городскую среду. Слой межотраслевых функциональных элементов - формирует технологический каркас для непрерывного взаимодействия всех субъектов городского информационного пространства с едиными структурами обработки данных. Слой отраслевых функциональных элементов - оптимизирует информационные ресурсы электронного правительства для повседневных задач управления. Слой социотехнических функциональных элементов - предоставляет мобильность государственных и муниципальных услуг в цифровом профиле горожан. Компонентное соотношение городским информационных систем в рамках фундаментальных слоев платформы Умного города проиллюстрировано на рис. 2 [6, 7].

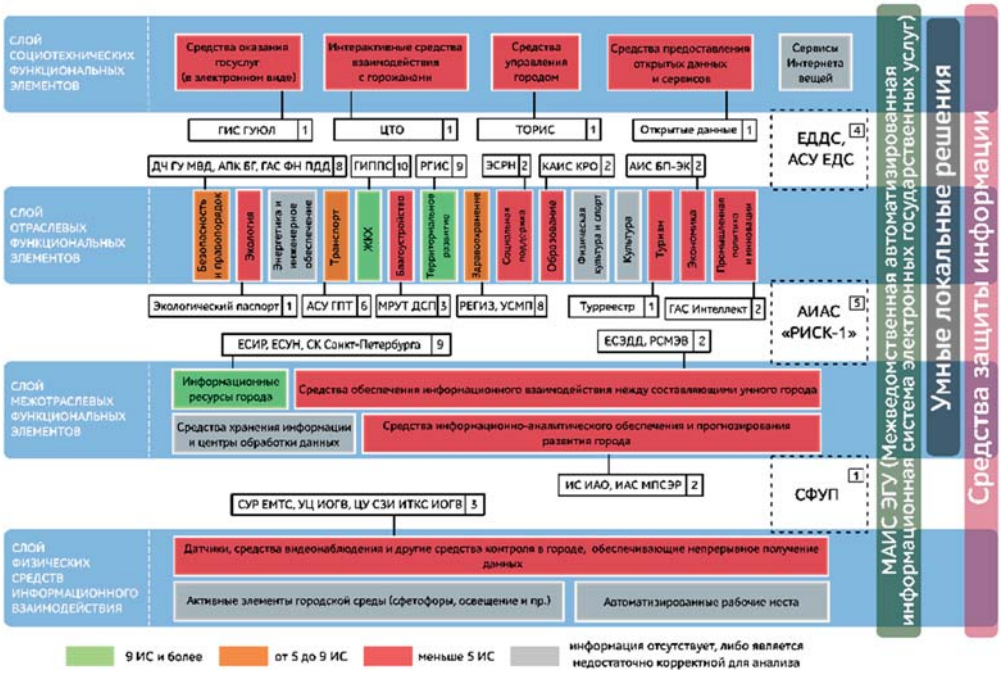


Рис. 2. Текущая ситуационная схема состояния ИТ-инфраструктуры

Важной составляющей ИТ-инфраструктуры города являются технологии функционирования систем и структуры обработки данных. Исходя из того, что данные обрабатываются и хранятся на платформе программных интеграционных решений, за основу был взят следующий анализ взаимосвязей целого инструментария (ОС-СУБД-ПО). Базовые аспекты межсистемного взаимодействия модульно показаны на рис. 3.

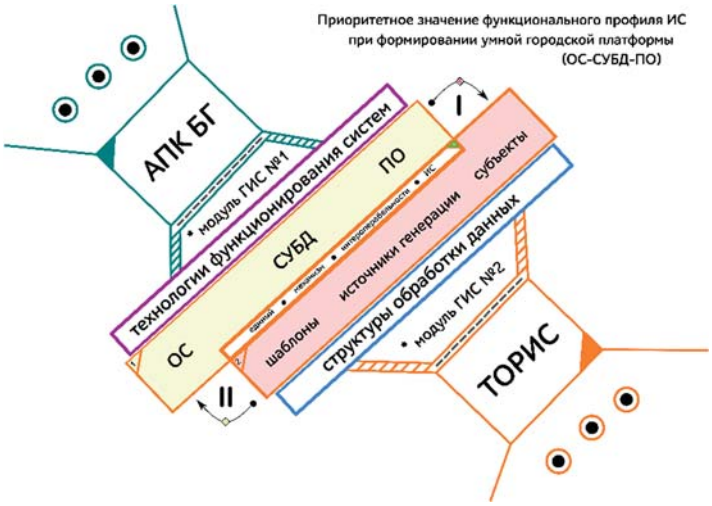


Рис. 3. Базовые аспекты межсистемного взаимодействия

Для начала анализа связанных систем была выстроена цепочка условных межсистемных запросов. По следующим направлениям: городская безопасность, электронные услуги и открытые данные. Для этого были выбраны системы по аналогичному профилю в каждом функциональном слое городской смарт-платформы. Формирование примера запроса упростит понимание алгоритма интероперабельности для повседневного обмена данными в государственных системах. Рассматривалась логика запросов от нижнего уровня взаимодействия к конечной системе. Таким образом, оценивается совместимость двух конкретных систем и общая структура запроса для всех участвующих систем. Поэтапный анализ позволил максимально детализировать каждый уровень и компонентную базу систем. Исходным источником данных является городская система Санкт-Петербурга - Реестр государственных информационных систем. Анализ данных применяется к современным программным и технологическим решениям, которые используются для обеспечения бесперебойного взаимодействия систем друг с другом [8, 9].

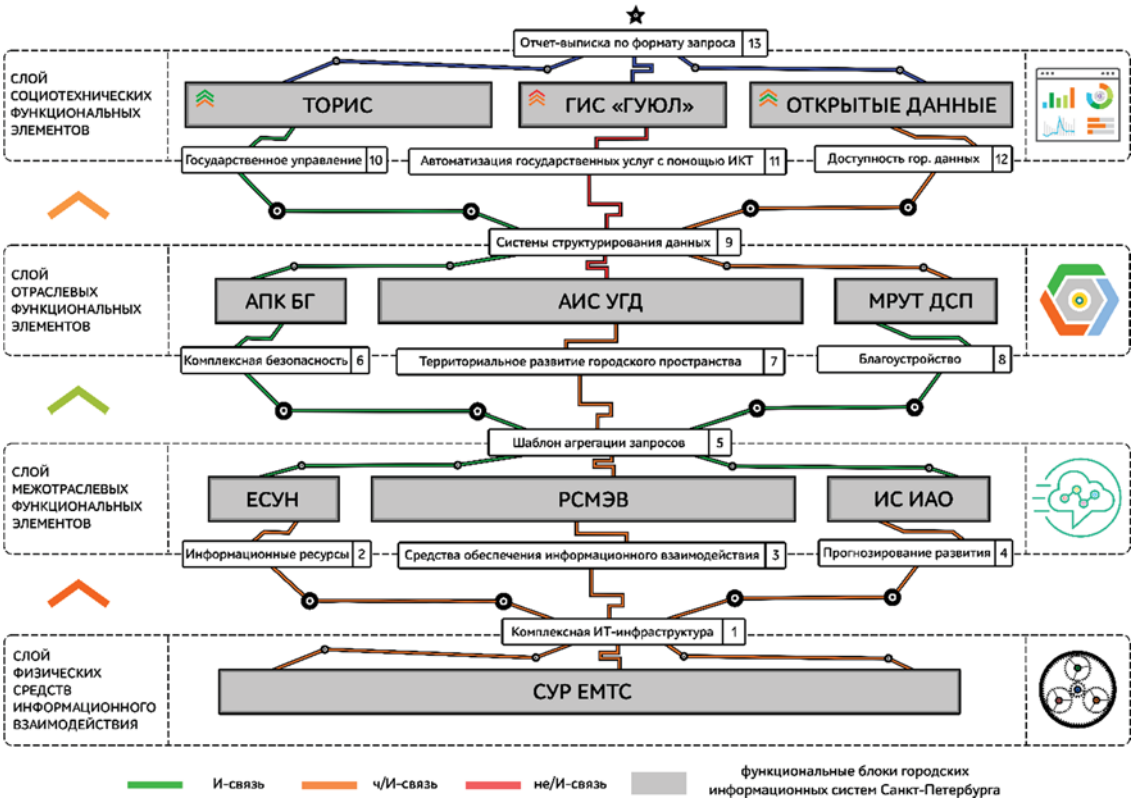


Рис. 4. Цепочка межсистемных запросов (по слоям функциональной платформы умного города)

Для упрощения понимания предлагаемого метода и детализации его расчета была выбрана схематическая визуализация согласно установленной архитектуре.

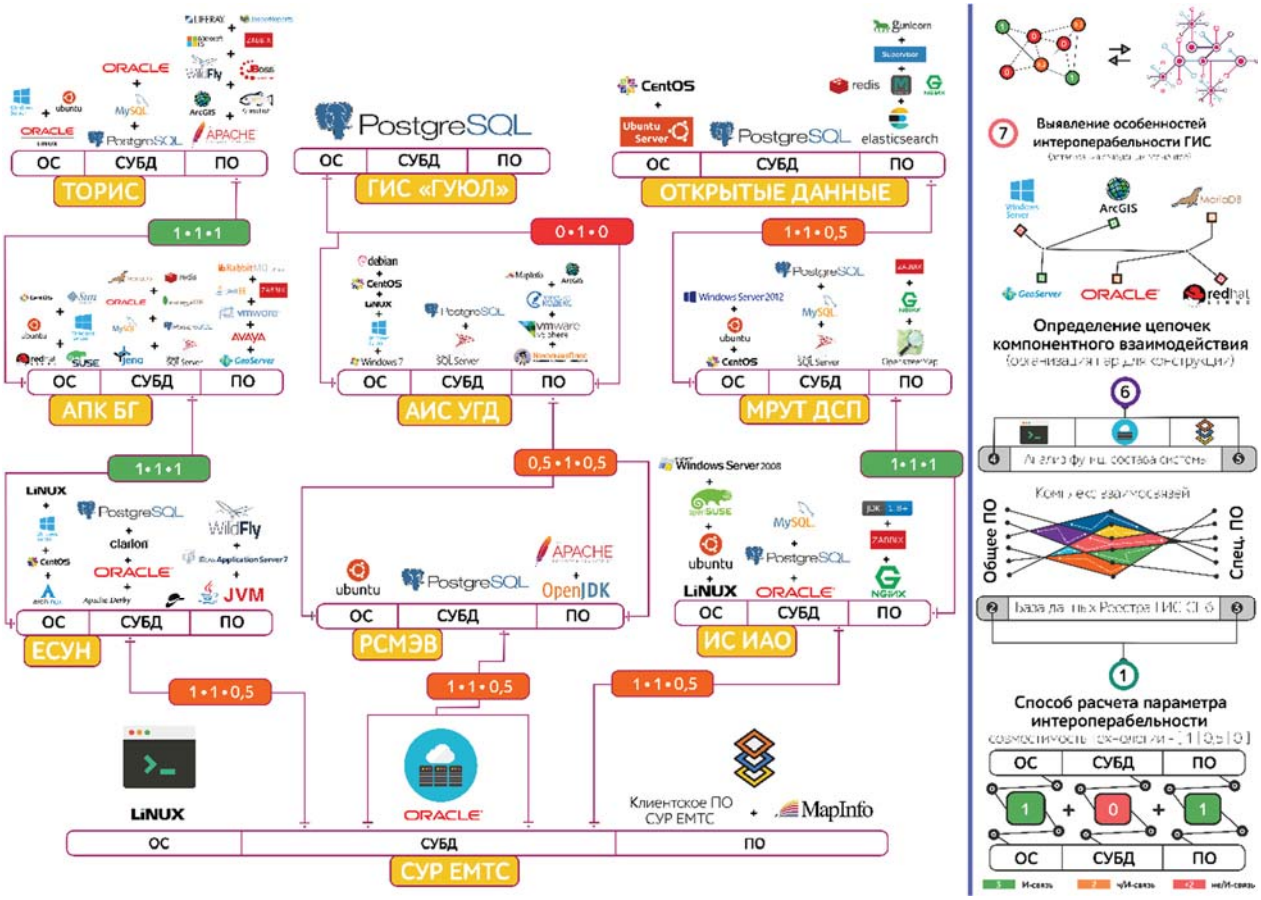


Рис. 5. Структурные анализ совместимости систем по приоритетным принципам методом «ОС-СУБД-ПО»

Основным принципом анализа являлось сравнение технологий «1к1» и их количественная оценка по результатам совместимости. Для устранения конфликта при оценке интероперабельности был введен пограничный параметр (0,5). Используется при недостаточности данных по конкретному технологическому решению или необходимости подключения к системе дополнительного модуля для реализации полного цикла взаимодействия.

В целом, по результатам исследования, практически все исследуемые системы прошли минимальный уровень функциональной интероперабельности. Некоторые моменты несовместимости связаны с неоднородностью ИТ-инфраструктуры (наличием отличающихся технологических решений у конкурирующих между собой поставщиков экосистем) [10, 11].

Стратегическая перспектива создания единой цифровой платформы города предполагает модульный подход к проектированию ИТ-инфраструктуры. В связи с этим рекомендуется использовать открытые архитектуры для более гибкой конфигурации сетевого взаимодействия к масштабу городских процессов [12].

Заключение. В статье рассматриваются основные проблемы городской ИТ-инфраструктуры и предлагается подход к её изучению. Подход основан на качественной сравнительной оценке совместимости систем и может быть применен для первичной оценки всех городских информационных систем. Такой способ исследования может быть дополнительно расширен количественными методами. Рассмотренный метод анализа информационных систем может стать основой для дальнейшей модернизации городской ИТ-инфраструктуры с целью внедрения технологий умного города.

СПИСОК ЛИТЕРАТУРЫ

1. Брауде-Золотарев М. и др. Интероперабельность информационных систем //Сборник материалов. – М.: INFOFOSSRU. – 2008.
2. Angula N., Dlodlo N. Towards a Framework to Enable Semantic Interoperability of Data in Heterogeneous Health Information Systems in Namibian Public Hospitals //International Conference on Information Theoretic Security. – Springer, Cham, 2018. – С. 835-845.
3. Реестр государственных информационных систем Санкт-Петербурга [Электронный ресурс]. - Режим доступа: https://reestr-gis.spb.ru/rgis/#gis (дата обращения 19.11.2018).
4. Cestari J. M. A. P., Loures E. F. R., Santos E. A. P. A Method to Diagnose Public Administration Interoperability Capability Levels Based on Multi-Criteria Decision-Making //International Journal of Information Technology & Decision Making. – 2018. – Т. 17. – №. 01. – С. 209 - 245.
5. Daliya V. K., Ramesh T. K. A survey on enhancing the interoperability aspect of IoT based systems //2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon). – IEEE Conferences, 2017. – С. 581 - 586.
6. Delgado J. C. M. Interoperability Frameworks for Distributed Systems //Encyclopedia of Information Science and Technology, Fourth Edition. – IGI Global, 2018. – С. 6566 - 6578.
7. Doan A. H., Halevy A., Ives Z. Principles of data integration. – Elsevier, 2012. – С. 520.

8. Gottschalk P. E-Government Interoperability and Information Resource Integration: Frameworks for Aligned Development: Frameworks for Aligned Development. – IGI Global, 2009. – С. 298.
9. IDABC E., Industry D. G. European interoperability framework for pan-European e-government services //European Communities. – 2004. – С. 1 - 26
10. Fonou-Dombeu J. V., Huisman M. A semantic-enabled framework for e-government systems development //Computer Systems and Software Engineering: Concepts, Methodologies, Tools, and Applications. – IGI Global, 2018. – С. 501 - 518.
11. Guijarro L. Interoperability frameworks and enterprise architectures in e-government initiatives in Europe and the United States //Government Information Quarterly. – 2007. – Т. 24. – №. 1. – С. 89 - 101.
12. IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces //IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003). – IEEE Standards, 2018. – С. 1 - 138.

ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ИНФОРМАТИКИ И ИНФОРМАТИЗАЦИИ

УДК 004.087

НЕКОТОРЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ РАДИОЧАСТОТНЫХ МЕТОК НА ПОВЕРХНОСТНЫХ АКУСТИЧЕСКИХ ВОЛНАХ

Верзун Наталья Аркадьевна, Колбанев Михаил Олегович, Омельян Александр Владимирович
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, omers27@mail.ru

Аннотация. Статья посвящена перспективной технологии создания различных приложений интернета вещей – технологии радиочастотной идентификации. Рассматриваются особенности функционирования RFID систем на поверхностно-акустических волнах, в частности, применяемые в подобных системах алгоритмы разрешения коллизий.

Ключевые слова: радиочастотная идентификация объектов; радиочастотная метка; интернет вещей; алгоритм антиколлизии; корреляционный алгоритм антиколлизии.

SOME ASPECTS OF THE USE OF RFID TAGS SURFACE ACOUSTIC WAVE

Verzun Natalia, Kolbanev Mikhail, Omelyan Alexander
Saint-Petersburg State University of Economics
21 Sadovaya Str., St. Petersburg, 191023, Russia
e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, omers27@mail.ru

Abstract. The article is devoted to the promising technology of creating various applications of the Internet of things – radio frequency identification technology. The features of functioning of RFID systems on surface-acoustic waves are considered, in particular, the collision resolution algorithms used in such systems.

Keywords: radio-frequency identification of objects; radio-frequency label; Internet of things; anti-collision algorithm; correlation anti-collision algorithm.

Введение.

Технология радиочастотной идентификации (RFID – Radio Frequency IDentification), основные принципы функционирования которой были разработаны еще в прошлом веке [1], в настоящее время, в связи с цифровой трансформацией реальной экономики, переживает всплеск интереса к ней. Системы контроля и управления доступом; инвентаризация, сортировка, регистрация различных предметов (багаж, почтовые отправления, биоматериал, музейные экспонаты и т. п.); логистика и цепочки поставок; профилактическое обслуживание и контроль целостности технических систем; идентификация беспилотных транспортных средств; отслеживание миграции животных; борьба с контрафактной продукцией – вот далеко не полный и постоянно пополняющийся перечень сфер применения RFID.

Существенное влияние на подъем популярности технологии радиочастотной идентификации оказало возникновение и развитие концепции интернета вещей (IoT – Internet of Things) [2]. Практическая реализация приложений IoT в различных областях человеческой деятельности ведет не только к огромному разнообразию умных вещей, но и к лавинообразному росту их числа, а ведь каждую вещь необходимо каким-то образом отличать от другой, т.е. идентифицировать. Последнее обстоятельство во многом и обусловило возросшую потребность в технологии RFID, которая обладает рядом преимуществ по сравнению с другими технологиями идентификации, возможными к применению в реальном мире: штриховые коды, системы на основе биометрических признаков [3].

Широко востребованная сегодня технология RFID нуждается в дальнейшем развитии и доработке для удовлетворения специфики интернета вещей в направлениях, например:

- уменьшения размеров радиочастотных меток и увеличение их срока службы;
- снижение стоимости всех аппаратных компонентов;
- увеличения скорости считывания;
- усовершенствования алгоритмов функционирования RFID систем;
- и пр.

В состав RFID систем входят следующие неотъемлемые элементы: радиочастотные метки, прикрепленные тем или иным образом к объектам идентификации; считыватели, связанные с метками по радиоканалу; и информационные системы для управления всеми процессами. Производство аппаратных компонентов, а также создание и внедрение

RFID систем представляет собой сложный процесс, в котором задействованы многие наукоемкие области знания: электротехника, микроэлектроника, электродинамика, радиотехника, радиосвязь и пр.

В RFID системах нашли применение 2 типа радиочастотных меток, имеющих значительные различия при производстве и эксплуатации: пассивные и активные (подробный обзор и классификацию меток см. [3]). Принципиальное их отличие состоит в том, что активная RFID метка содержит однокристальный микроконтроллер (чип), а пассивная нет. Программное обеспечение, прошитое в микроконтроллер активной метки, способно реализовывать сложные протоколы взаимодействия как со считывателем, так и с другими метками. Различны эти два типа меток и с точки зрения получения питания: активная метка получает энергию, необходимую для обработки команд считывателя и формирования ответного сигнала, от встроенной батареи, а пассивная метка – по радиолинии от устройства считывания.

В отличие от активных, пассивные метки [3] обладают, в частности, следующими особенностями: не требуют встроенного источника питания и, как следствие, имеют почти не ограниченный срок службы и меньший вес и размеры (большую часть метки составляет встроенная антенна); допускают только считывание данных с них; применяют в работе поверхностно-акустические волны (ПАВ) [4]. Малый вес и габариты, а также большой срок эксплуатации пассивных меток на ПАВ превращает RFID системы, основанные на их использовании, в одну из наиболее перспективных технологий создания различных приложений IoT.

Структура метки на ПАВ представлена на рис.1 [5].

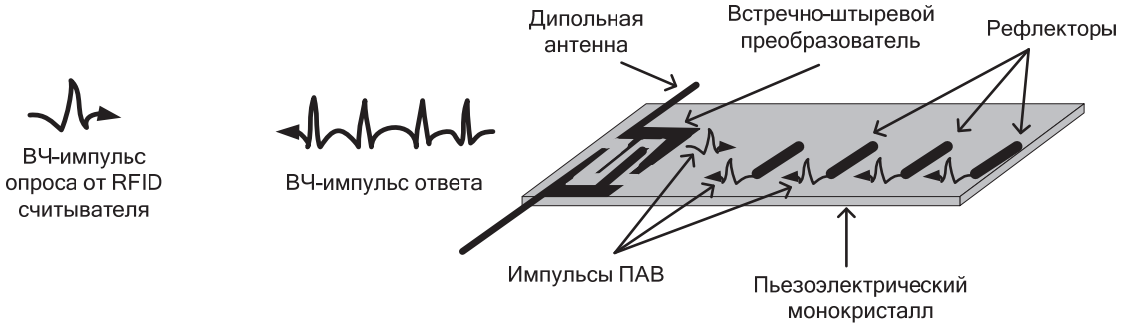


Рис.1. RFID метка на ПАВ

В основе технологии RFID меток на ПАВ лежат физические процессы прямого и обратного пьезоэлектрического эффекта. Прямой пьезоэлектрический эффект – возникновение поляризации диэлектрика под механическими воздействиями. Подобный диэлектрик называется пьезоэлектриком. Обратный пьезоэлектрический эффект – возникновение механических деформаций под действием электрического поля.

По сути, пьезоэлектрик позволяет преобразовывать механическую энергию в электрическую и, наоборот, электрическую в механическую. ПАВ – это упругие волны, распространяющиеся вдоль поверхности твердого тела. В пьезоэлектрике их можно инициировать электрическим импульсом.

Как видно из рис.1 дипольная антенна каждой метки, подключенная к встречно-штыревому преобразователю (ВШП), принимает высокочастотный (ВЧ) сигнал опроса от RFID-считывателя. Электрический сигнал, выработанный ВШП из отраженной волны, преобразуется антенной метки в ВЧ последовательность электромагнитных импульсов (ВЧ импульс ответа), которая излучается в эфир. ВЧ импульс ответа может приниматься антенной считывателя – это код (или уникальный идентификатор) метки, который закладывается в ее топологии при изготовлении и не может меняться на протяжении всего срока службы.

Типовая RFID система с метками на ПАВ, показана на рис.2.

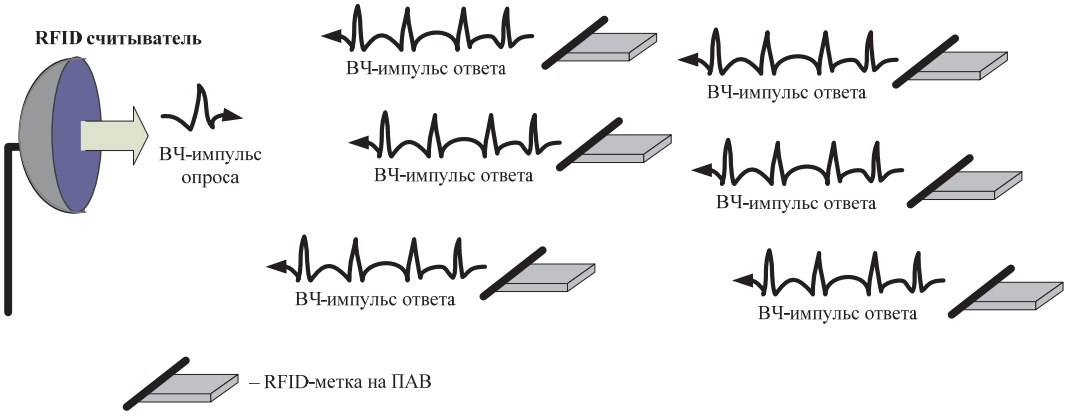


Рис.2. RFID система

Предполагается, как правило, что в зоне действия одного считывателя расположено несколько меток и все они одновременно формируют и передают свои ответы (уникальные идентификаторы), реагируя таким образом

на ВЧ импульс опроса [5]. Если не предпринять специальных мер, подобная ситуация приводит к коллизии (или конфликту) радиочастотных меток [6], т.е. к тому, что происходит наложение ответных сигналов от нескольких меток друг на друга, и в результате происходит искажение данных, принимаемых считывателем [7]. Для разрешения ситуации коллизии в системах радиочастотной идентификации используют специальные антиколлизионные алгоритмы.

Выбор алгоритма устранения коллизий в RFID системах определяется: функциональными возможностями непосредственно самих меток и предварительными знаниями считывателя о тех или иных свойствах радиочастотных меток (серийные номера, расстояние до считывателя, место расположения и т.п.).

Так, например, для активных меток с чипами может быть организовано взаимодействие со считывателем по определенному протоколу, позволяющее осуществлять продуктивную передачу (для случая активной метки чтение и запись) данных без взаимного искажения радиосигналов разных меток. В данном случае возможны к применению случайные, детерминированные, пространственные и корреляционные алгоритмы антиколлизии [7]. Первые два типа (случайные и детерминированные) предполагают либо диалог метки со считывателем, либо самостоятельное принятие решений радиочастотной меткой, но в любом случае без встроенного микроконтроллера не обойтись. А вот пространственные и корреляционные алгоритмы могут найти свое применение в RFID системах как с активными, так и с пассивными метками.

Пространственные алгоритмы антиколлизии основаны на выборе такого взаимного размещения множества меток и считывателя, которое позволяет направить ВЧ-импульс опроса только к одной определенной метке и не инициировать при этом считывание данных с других меток. В результате происходит поочередное считывание уникальных кодов меток. Подобный последовательный опрос меток может быть обеспечен также путем изменения дополнительных параметров: мощности сигнала опроса, его направленности. Хороший антиколлизионный эффект при применении пространственного алгоритма достигается в том случае, когда есть возможность измерить расстояние до каждой метки, находящейся в зоне опроса RFID-считывателя, что позволяет организовать последовательное чтение кодов меток.

Однако применение пространственных алгоритмов затрудняется по мере увеличения числа меток, плотности их распределения и, соответственно, уменьшения расстояния между соседними метками, т. к. в этом случае усложняется достижение требуемой точности измерения расстояния от считывателя до метки.

На практике пространственные алгоритмы хорошо показывают себя в таких случаях, когда:

– считыватель имеет низкую мощность сигнала опроса и считывает данные с метки, находясь на малом расстоянии от нее;

– совокупность меток представляет собой статическую систему, в которой точно известно положение всех опрашиваемых меток, так что можно заранее определить зону опроса при каждом положении считывателя;

– пространственные алгоритмы применяются в сочетании с другими алгоритмами антиколлизии, например, корреляционными.

Корреляционные алгоритмы антиколлизии основаны на использовании процедур вычисления взаимнокорреляционной функции (ВКФ) и автокорреляционной функции (АКФ) сигналов, излучаемых метками на ПАВ [7] для выделения искомого сигнала отклика (кода метки) из радиоэфира. Очевидно, что код искомой метки при этом должен быть известен считывателю заранее.

Корреляция двух сигналов $S_1(t)$ и $S_2(t)$ это результат их энергетического взаимодействия, в итоге которого возникает новый сигнал, описываемый ВКФ. ВКФ характеризует степень связи между сигналами, сдвинутыми на время жизни сигнала τ:

$$U_{S_1S_2}(\tau) = \int_0^{\tau} S_1(t)S_2(t+\tau)dt \qquad (1)$$

Если сигналы $S_1(t)$ и $S_2(t)$ синхронны, то ВКФ вырождается в число:

$$U_{S_1S_2} = \int_0^{\tau_0} S_1(t)S_2(t)dt \qquad (2)$$

Если сигналы независимы, то их взаимнокорреляционная функция $U_{S_1S_2} = 0$. В данном случае говорят, что сигналы ортогональны.

АКФ характеризует степень связи между сигналом и его сдвинутой на некоторое время копией. В синхронном случае автокорреляционная функция равна энергии сигнала:

$$E = \int_0^{\tau_0} S(t)^2 dt \qquad (3)$$

Одно из значимых свойств радиочастотных меток на ПАВ заключается в следующем: если сигнал опроса от RFID-считывателя сформировать как зеркальную последовательность кода метки, образованного рефлекторами (см. рис.1), то за счет корреляции отраженный импульс метки, будет импульсом значительной амплитуды, и соответственно, наоборот, уменьшение ВКФ сигнала опроса с кодом метки приводит к уменьшению амплитуды отклика.

Следовательно, для устойчивой работы RFID системы на ПАВ (т.е. гарантированного распознавания радиочастотных меток) необходимо подбирать такую совокупность кодовых комбинаций для идентификации меток, которые попарно будут имеют достаточно маленькую ВКФ. Наилучший вариант – применение в RFID системе совокупности кодов, состоящей только из ортогональных кодов, т. е. таких, для которых ВКФ любой пары ее кодов равна 0.

Такими свойствами обладают, например, коды Р. Баркера [8], предложенные еще в 1953 году и нашедшие свое применение в цифровых системах цикловой (кадровой) синхронизации [9]. Однако известно только девять кодовых двоичных последовательностей Баркера длиной 2, 3, 4, 5, 7, 11 и 13 символов (по 2 последовательности длиной 2 и 4 символа), что явно недостаточно для практического создания RFID систем.

Ортогональные коды можно получить при помощи функций Уолша, для записи которых служит матрица Адамара [10]. Это группа из 2^n функций, которая формируется рекуррентно по следующей общей схеме:

$$H_{2^n} = \begin{bmatrix} H_{2^{n-1}} & H_{2^{n-1}} \\ H_{2^{n-1}} & -H_{2^{n-1}} \end{bmatrix} \quad (4)$$

Коды по строкам и по столбцам ортогональны. Корреляция строки с самой собой дает 2^n, с любой другой – 0. Свойства полученных таким образом кодов сохраняются только при отсутствии временного сдвига получаемых сигналов, что ограничивает их использование только синхронными системами, т.е. когда есть возможность определить момент времени начала вычисления ВКФ. Функции Уолша нашли свое применение в системах радиосвязи основанных на кодовом разделение каналов, (например, в стандартах сотовой связи CDMA2000, UMTS), но вот применение их в RFID системах ограниченно.

Заключение.

Технология радиочастотной идентификации в настоящее время в связи с цифровой трансформацией реальной экономики, переживает всплеск интереса к ней. Такие достоинства радиочастотных меток на ПАВ как малый вес и габариты, неограниченный срок эксплуатации и др. превращает RFID системы, основанные на их использовании, в одну из наиболее перспективных технологий создания различных приложений IoT.

Для устойчивой работы RFID системы на ПАВ необходимо подбирать такую совокупность кодов для идентификации меток, которые попарно будут имеют достаточно маленькую ВКФ. Наилучший вариант – совокупность, образованную только ортогональными кодами. Количество кодов, которое может быть получено с применением известных на сегодня подходах, не позволяет создать RFID систему с востребованным на практике числом меток.

СПИСОК ЛИТЕРАТУРЫ

1. Верзун Н. А., Колбанёв М. О., Омельян А. В. RFID-технологии для эффективности и безопасности документооборота // Технологии информационно-экономической безопасности: сб. ст. сотр. каф. ИС и Т. СПб.: Изд-во СПбГЭУ, 2016. С.44–51.
2. Верзун Н. А., Ипатов О.С., Колбанёв М. О. Интернет вещей и информационно-технологическая безопасность // Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. СПб.: Изд-во СПбГЭУ, 2016. С.22–29.
3. Верзун Н. А., Воробьева Д. М., Колбанёв А. М., Колбанёв М. О. Обзор технологий и стандартов RFID систем // Информационные технологии и телекоммуникации. 2018. Том 6. № 1. С. 1–11.
4. Койгеров А. С., Забузов С. А., Дмитриев В. Ф. Исследование корреляционного метода для решения задачи антиколлизии для систем радиочастотной идентификации на ПАВ // Информационно-управляющие системы. 2009. № 5. С. 48–55.
5. Верзун Н. А., Колбанёв М. О., Омельян А. В. Введение в инфокоммуникационные технологии и сети Future Networks: учебное пособие. СПб.: Изд-во СПбГЭУ. 2016. 51 с.
6. Шарфельд Т. Системы RFID низкой стоимости / Под ред. С. Корнеева. М., 2006. 197 с. URL: http://www.alpha1.ru/recommend /rfid_lowcost.pdf.
7. Верзун Н. А., Воробьева Д. М., Колбанёв А. М., Колбанёв М. О. Корреляционные алгоритмы антиколлизии для RFID систем // Информационные технологии и телекоммуникации. 2018. Том 6. № 1. С. 82–91.
8. Варакин Л. Е. Системы связи с шумоподобными сигналами. М.: Радио и связь. 1985. 384 с.
9. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с англ. М. : Вильямс, 2007. 1104 с.
10. Беспалов М.С., Скляренко В.А. Дискретные функции Уолша и их приложения: учеб. пособие / Владим. гос. ун-т. им. А. Г. и Н. Г. Столетовых. Владимир: Изд-во ВлГУ, 2014. 68 с.

УДК 004.811

КОГНИТИВНЫЕ ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ ДЛЯ МОНИТОРИНГА

Водяхо Александр Иванович[1], Осипов Василий Юрьевич[2], Червонцев Михаил Александрович[2], Жукова Наталия Александровна[3]

[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия

[2] Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия В.О., 39, Санкт-Петербург, 199178, Россия

[3] Научно-инженерный центр Санкт-Петербургского электротехнического университета» (АО «НИЦ СПб ЭТУ»)
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Политехническая ул., 22К, Санкт-Петербург, 194021, Россия
e-mails: aivodyaho@mail.ru, osipov_vasiliy@mail.ru, chervontsev.mikhail@nicetu.spb.ru, nazhukova@mail.ru

Аннотация: В статье рассматриваются возможные подходы к использованию интеллектуальных технологий при построении систем мониторинга. Предлагается использовать когнитивные архитектуры для построения ГИС-ориентированных систем мониторинга. В основе предлагаемого подхода лежит идея автоматической генерации бизнес-процессов мониторинга. Использование предлагаемого подхода позволяет повысить скорость работы ГИС-ориентированных систем мониторинга и уменьшить стоимость их разработки.

Ключевые слова: мониторинг; ГИС; когнитивные архитектуры.

COGNITIVE GIS MONITORING SYSTEMS

Vodyaho Alexander[1], Osipov Vasiliy[2], Chervontsev Mikhail[3], Zhukova Natalia[2]
[1] Saint Petersburg Electrotechnical University «LETI»
5 Professor Popov Str., St. Petersburg, 197376, Russia
[2] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th liniya, Vasilievsky Island, St. Petersburg, 199178, Russia
[3] The Research and Engineering Center of the Saint Petersburg State Electro-Technical University (LETI)
22K Politechnicheskaya Str., St. Petersburg, 194021, Russia
e-mails: aivodyaho@mail.ru, osipov_vasiliy@mail.ru, chervontsev.mikhail@nicetu.spb.ru, nazhukova@mail.ru

Abstract: In the article possible approaches to usage of intelligent technologies for GIS based monitoring systems are discussed. It is suggested to use cognitive architectures for building GIS oriented monitoring systems. Suggested approach is based on the idea of automatic generation of monitoring business processes. Usage of suggested approach allows increase the speed of monitoring systems operation and reduce the cost of development.

Keywords: monitoring; GIS; cognitive architectures**.**

Введение.

Широкое распространение и применение геоинформационных систем (ГИС) при решении различных прикладных задач обусловлено удобством работы с ними конечных пользователей. Важным преимуществом ГИС является то, что они позволяют работать как с данными об объектах предметной области, так и с данными об окружающей среде. Долгое время ГИС развивались как системы графической визуализации пространственных (географических) данных и связанной с ними информации о необходимых объектах на картографической основе. В течение этого времени их функциональные возможности и сфера их применения постоянно расширялись. В настоящее время они находят применение при построении самых разных классов информационных систем (ИС).

Можно выделить, по крайней мере, 4 различных подхода к созданию ГИС-ориентированных ИС: 1) стандартная ГИС платформа является основой для построения ГИС-приложений, 2) ГИС является одним из сервисов визуализации, причем это не обязательно основной сервис, при этом для построения данного сервиса используется готовая платформа, 3) ГИС является основным средством визуализации для создаваемой ИС, при этом платформа адаптируется для нужд конкретной разработки, 4) ИС строится на базе ГИС платформы собственной разработки.

Магистральное направление развития ГИС технологий и поддерживающих их ГИС платформ связано с их интеллектуализацией. В качестве примера подобного подхода можно рассматривать интеллектуальную ГИС (ИГИС) [1-3], которая включает в свой состав многие средства искусственного интеллекта (ИИ). Следует заметить, что ИГИС в том виде как она описана в [2], в большей степени может рассматриваться как ГИС платформа общего назначения, чем как методология проектирования интеллектуальных ГИС, т.е. ИГИС в смысле [2] – это название конкретной платформы, а не множество технологий, использующих методы и средства ИИ для построения ГИС. ИГИС включают в свой состав многие средства ИИ. В частности, они могут включать машину логического вывода и экспертную систему, иерархию онтологий (баз знаний) предметной области, средства математического моделирования, имитационного моделирования на основе сценарного подхода, построения и исполнения сценариев в режиме реального времени с отображением на электронных картах, графической разработки иерархии онтологий и сценариев, проигрывания сценариев [2, 3]. В ряде случаев в состав ИГИС могут вводиться модули интеллектуальной поддержки принятия решений [2, 3]. В результате ИГИС оказываются способными к решению таких задач, как распознавание ситуаций, выявление причин их возникновения, прогнозирование их развития.

В настоящей статье рассматривается один из возможных подходов к построению одного из подклассов ИГИС – когнитивные ГИС мониторинга (КГИСМ).

Системы мониторинга

Понятие мониторинг в самом общем виде можно определить, как итерационный процесс, выполняющийся с целью получения, накопление и обработки данных, информации и (или) знаний о некоторой внешней системе (целевой системе, ЦС) и представление этих данных, информации, знаний заинтересованным сторонам в требуемой форме, в частности в ГИС форматах. Если результаты мониторинга используются для формирования управляющих воздействий для ЦС, то в этом случае имеем систему мониторинга и управления (СМУ). Система мониторинга в этом случае выступает как подсистема СМУ. Можно выделить, по крайней мере, следующие основные классы ЦС: социальные системы, биологические системы, природные системы, антропогенные

системы, гибридные системы. С точки зрения использования геоинформационных систем мониторинга (ГИСМ), наибольший интерес представляют природные и антропогенные ЦС. В качестве основных пользователей ГИСМ могут выступать самые разные специалисты: операторы, отвечающие за мониторинг технического состояния ЦС; специалисты по технической поддержке, аналитики, занимающиеся построением моделей; исследователи, менеджеры разного уровня, отвечающие за общие вопросы.

Современный этап развития информационных технологий характеризуется такими моментами как необходимость работать с очень большими объемами данных, постоянным изменением структуры ЦС и постоянным ужесточением требований, предъявляемых к стоимости и срокам разработки. Таким образом, возникают проблемы отслеживания состояния очень больших, территориально распределенных систем с постоянно изменяющейся структурой, что требует создания сложных и дорогостоящих систем мониторинга. Решение этой проблемы может быть найдено в использовании когнитивных систем мониторинга, т.е. систем мониторинга, построенных по принципу когнитивной системы.

Когнитивные системы

По своей задумке [4] когнитивные системы принципиально отличаются от традиционных ИС, включая интеллектуальные системы. В идеале, когнитивные системы не должны жестко программироваться, а должны управлять процессами мониторинга, задавая цели мониторинга, определять пути их достижения, оценивать результаты мониторинга. Для этого такие когнитивные системы мониторинга подобно человеку должны воспринимать данные от наблюдаемых объектов, выполнять их обработку, связывать их в пространстве и во времени, формировать и перестраивать модели объектов и процессов мониторинга на их основе.

В сильном варианте когнитивную ИС можно определить, как систему, которая решает задачи подобно тому, как их решает человек. В более слабом варианте – это система, которая, реализует элементы разумного поведения. Когнитивную систему мониторинга можно определить, как систему мониторинга, использующую в процессе функционирования модели ЦС, представленной виде знаний, что можно рассматривать как еще более слабое определение когнитивной системы.

В этом случае встает вопрос о выборе модели или моделей, которые могут быть положены в основу процесса когнитивного мониторинга. Модель когнитивного мониторинга должна удовлетворять 6 основным требованиям: модель должна поддерживать решение возможно большего числа задач мониторинга, в первую очередь, поддерживать модель логического вывода и работы в ГИС системах, модель должна работать с большими данными, модель можно легко модифицировать, модель можно синтезировать из данных, модель должна быть исполняемой.

Анализ известных моделей показал, что с помощью одной модели решить задачу не удается. Предлагается использовать множество моделей, которые можно преобразовывать посредством использования сервисов трансформации моделей. В качестве базовой модели выбрана автоматная модель – многоуровневые относительно конечные операционные автоматы [5].

Обобщенная модель функционирования КГИСМ

В самом общем виде функционирование КГИСМ может быть описано в терминах модели слияния данных (Data Fusion) широко известной как JDL модель [6], которая включает 6 уровней (рис. 1). Каждому из них ставится в соответствие определенная функциональность на достаточно высоком уровне.

Данные, информация и знания поступают от источников. Источники могут быть локальными, распределенными и внешними. В качестве источников могут выступать датчики, базы данных и знаний.

Уровень 0. Определение характеристик отдельных сигналов (Signal/Feature Assessment). Основная задача, решаемая на этом уровне – это оценка и предсказание значений отдельных параметров. Можно говорить, что на этом уровне осуществляется обработка данных, относящихся к отдельным частям объектов. В зависимости от предметной области это может быть обработка изображений на уровне пикселов, очистка сигнала от шумов и помех и т.п.

Уровень 1. Оценка характеристик отдельных объектов (Entity assessment). Основная задача, решаемая на этом уровне – это оценка и предсказание значений отдельных параметров и состояния отдельных сущностей (объектов). При этом реализуются функции, связанные с формированием информации об отдельных объектах. Это делается на основе информации об элементах объектов. Это может быть, например, информация о месте нахождения объекта, скорости перемещения и направлениях движения, либо информация о техническом состоянии отдельных узлов сложной технической системы.

Уровень 2. Оценка ситуации (Situation Assessment). Основная задача, решаемая на этом уровне – это оценка и предсказание состояния структуры и параметров отношений между сущностями некоторой части реального мира и их влияние на состояние самих объектов. На этом уровне реализуются функции, связанные с формированием информации о ситуации в определенном контексте в терминах сущностей, отношений между сущностями и событий.

Уровень 3. Определение реакции (Impact Assessment). Основная задача, решаемая на этом уровне – это оценка и предсказание будущих состояний системы и ее частей в терминах полезность/стоимость, формирование альтернативных вариантов реакции системы. На этом уровне осуществляется оценка ситуации, которая может включать оценку динамики развития ситуации, предположения о возможных действиях друзей и врагов, угрозах и собственных уязвимостях.

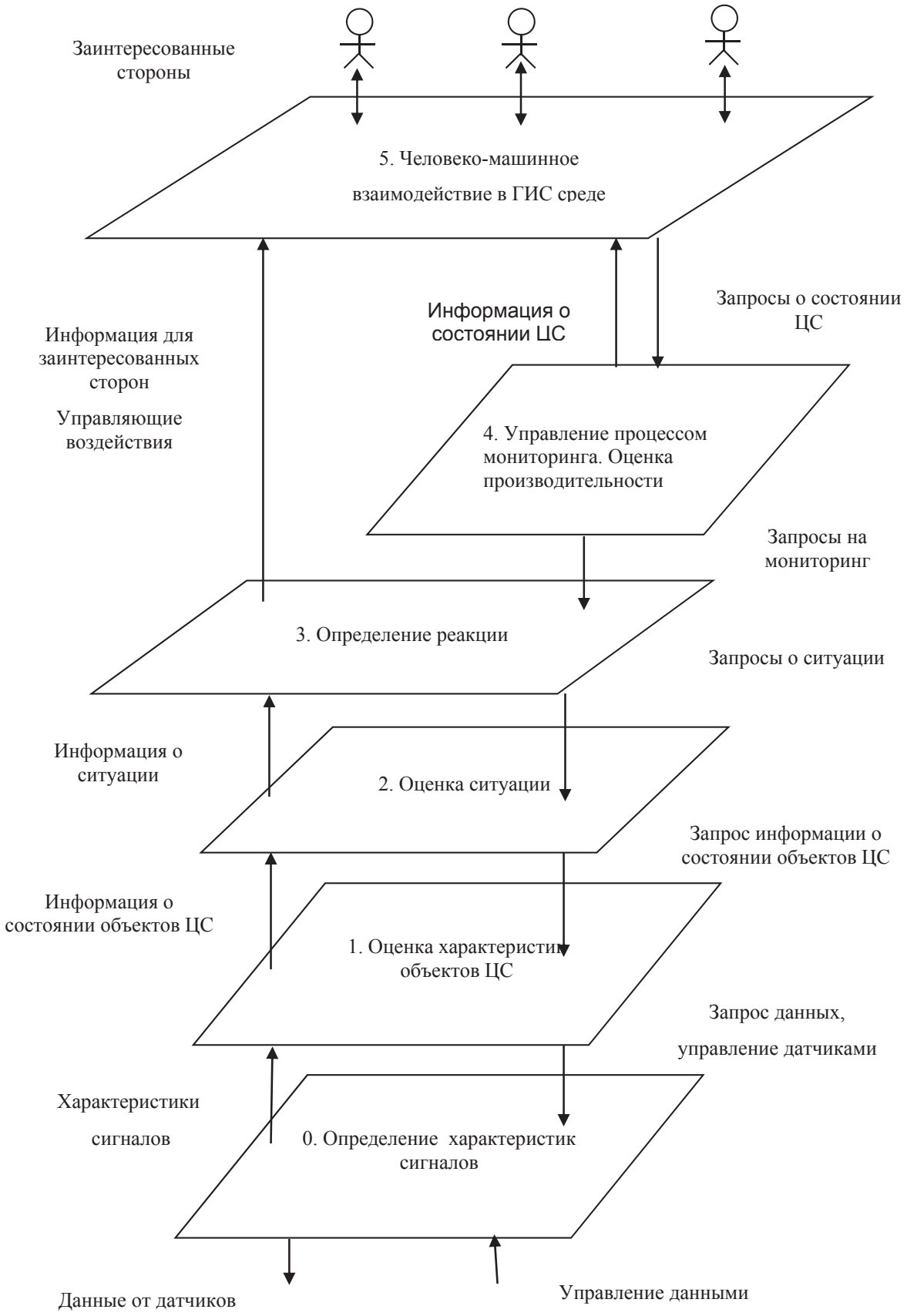


Рис. 1. Процессы, реализуемые в КГИСМ

Уровень 4. Управление процессом мониторинга. Оценка производительности (Process Management and Assessment). Основная задача, решаемая на этом уровне, – это оценка бизнес-процесса мониторинга и предсказание характеристик производительности самой системы и их сравнение с желаемыми показателями

эффективности. На этом уровне, в частности, реализуются функции мониторинга самого процесса, например, с целью улучшения временных характеристик.

Уровень 5. Человеко-машинное взаимодействие (Cognition Refinement). На этом уровне реализуются функции, связанные с совершенствованием человеко-машинного интерфейса. Этот уровень отвечает за виртуализацию и коллективное принятие решений. На данном уровне реализуются механизмы управления знаниями, в частности, определяется кто запрашивает информацию, кто имеет доступ к той или иной информации, для чего будет использована информация и определяется в каком виде и в каком объеме она должна быть представлена заинтересованному лицу.

Предполагается, что в рамках JDL модели реализуется двунаправленный процесс (рис. 1). Снизу-вверх и сверху вниз. Движение снизу-вверх это выделение информации из данных, а затем выделение знаний из информации и принятие решений.

Движение сверху вниз – это поток запросов, которые формулируются заинтересованными лицами в терминах предметной области. Запросы трансформируются на запросы информации, которые в свою очередь, трансформируются в запросы на получение данных.

Отдельный контур образует процесс управления ресурсами самой системы, который включает оценку качества функционирования системы и управление ресурсами с целью повышения качества функционирования самой системы.

Когнитивная машина мониторинга

Основой КГИСМ является когнитивная машина мониторинга (КММ), которая может рассматриваться либо как архитектурный фреймворк, либо как платформа, либо как среда проектирования КГИСМ. КММ представляет собой набор сервисов разного уровня, которые могут использоваться для построения конкретных экземпляров КСМ. Концептуальная структура КММ показана на рис. 2.

В состав КММ входят 7 основных подсистем:

1) модуль построения моделей (Model Mining Module, MMM),
2) модуль трансформации моделей (Model Transformation Module, MTM),
3) модуль обработки моделей (Model Processor, MP),
4) генератор архитектур,
5) генератор ГИС представлений,
6) репозитарий,
7) набор адаптеров.

MMM – это модуль, который отвечает за построение и поддержание моделей в актуальном состоянии. MTM – это модуль, который отвечает за приведение моделей к нужному представлению. PM – это модуль, который отвечает за процессинг моделей, в частности, реализует рассуждения на моделях, генератор архитектур формирует загружаемые модули и используется при работе с динамическими архитектурами. Репозитарий предназначен для хранения моделей, данных и знаний. Генератор отчетов и реакций выполняет несколько функций. В режиме ручного управления он выдает информацию о состоянии ЦО для ЛПР. В режиме автоматического управления он выдает управляющие воздействия на СМ и на ЦО. В случае использования динамической загружаемой архитектуры, этот модуль отвечает также за загрузку архитектурных модулей в распределенную среду КГИСМ. Адаптеры используются для поиска информации и знаний во внешних источниках.

КММ функционирует следующим образом. На вход КММ поступают данные мониторинга. Если модель неизвестна или требует уточнения и (или) верификации, то для этого используется MMM. Типовой режим- это проверка текущих моделей на актуальность и перестройка моделей при поступлении сообщений о наступлении некоторых событий. Местом хранения моделей является репозитарий.

Принятие основных решений реализуется на уровне моделей, которые строятся в терминах знаний. Для этого из входного потока данных требуется извлечь знания. Эту процедуру реализует MMM в состав которого входят сервисы более низкого уровня, которые позволяют извлекать знания из данных и событий. Этот процесс строится в соответствии с JDL моделью [6, 7]. MP выполняет функцию процессора, к которому можно обращаться с запросами на SPARQL. Генератор ГИС представлений выполняет 3 основные задачи. При работе в ручном режиме он выдает ЛПР информацию, необходимую ему для принятия решений. При работе в автоматическом режиме генератор самостоятельно формирует управляющие воздействия, как для управления когнитивной сетью, так и для управления ЦО, например, с целью реконфигурации.

Если в рамках КММ реализуется динамическая архитектура, то генератор архитектур синтезирует требуемые модули. Такое решение может быть актуально, например, в случае, когда требуется сгенерировать тестовую процедуру для заданной конфигурации. Если структура обслуживаемого ЦО известна и мало изменяется, то загружаемые модули могут храниться в библиотеках, которые находятся в репозитарии. Использование загружаемых архитектур (on demand) актуально, прежде всего, для туманных структур, когда ресурсы модулей промежуточного уровня ограничены.

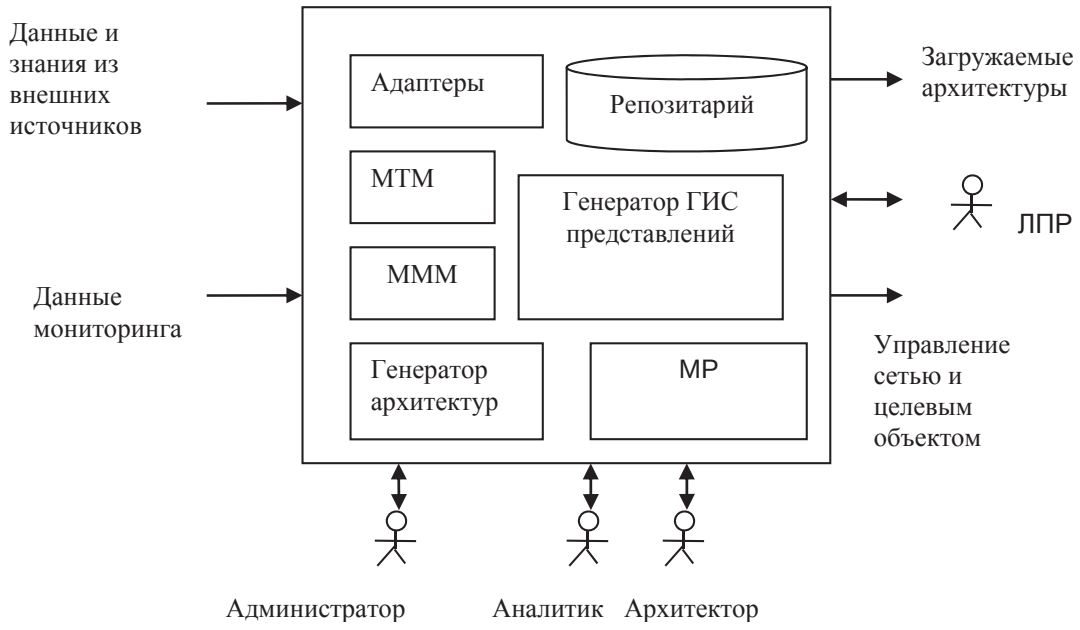


Рис. 2. Когнитивная машина мониторинга

Заключение.

В результате проведенных исследований предложен подход к построению ГИС ориентированных систем мониторинга, отличительной особенностью которого является использование когнитивного подхода. В качестве обобщенной модели предлагается использовать модель слияния данных (JDL модель). Когнитивные возможности реализуются посредством использования когнитивной машины.

СПИСОК ЛИТЕРАТУРЫ

1. Burrough, P. A. and McDonnell, R. A. (1998). Principles of geographical information systems. Oxford University Press, Oxford, 327 pp.
2. Интеллектуальные географические информационные системы для мониторинга морской обстановки // Под общ. ред. чл.-кор. РАН Юсупова Р.М. и д-ра тех. наук Поповича В.В. - СПб.: Наука, 2013. - 284 с.
3. Smirnova O., Tsvetkov M., Sorokin R Intelligent GISfor Monitoring and Prediction of Potentially Dangerous Situations. International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management, SGEM 14. 2014. С. 659-666.
4. World survey of artificial brains. Part II: Biologically inspired cognitive architectures / B. Goertzel, R. Lian, I. Arel, H. de Garis, S. Chen // Neurocomputting.2010. doi:10.1016/j.neucom.2010.08.012.
5. Осипов В.Ю. Синтез результативных программ управления информационно-вычислительными ресурсами // Приборы и системыуправления. 1998. №12. С.24-27
6. Blasch E., Bosse E, Lambert D. High-Level Information Fusion Management and System Design, Artech House Publishers, Norwood, MA. 2012
7. Handbook of multisensor data fusion. Theory and practice. Second edition. Edited by Martin E. Liggins, David L. Hall, James Llinas. CRC Press. Taylor & Frances Group. 2009, pp. 849.

УДК 004.942:004.728.4

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ЗОНДОВОГО ПРОТОКОЛА МАРШРУТИЗАЦИИ ДЛЯ MANET СЕТЕЙ В СРЕДЕ МАТЛАБ

Дорогов Александр Юрьевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: vaksa2006@yandex.ru

Аннотация. Рассмотрена имитационная модель зондового протокола маршрутизации для использования в беспроводных сетях с динамически изменяемой топологией. Описаны принципы построения имитационной модели в программной среде МАТЛАБ. Представлены результаты моделирования сети для различных вариантов параметров протокола. Исследованы особенности зондового протокола. Показана необходимость оптимального выбора узла запуска зондов для уменьшения времени сходимости алгоритма маршрутизации. Исследована помехоустойчивость протокола маршрутизации.

Ключевые слова: маршрутизация; протокол; имитационная модель; беспроводные сети; MANET.

SIMULATION OF PROBE ROUTING PROTOCOL FOR WIRELESS NETWORKS IN THE ENVIRONMENT OF MATLAB

Dorogov Alexander
Saint Petersburg Electrotechnical University «LETI»
5 Professor Popov Str., St. Petersburg, 197376, Russia
e-mail: vaksa2006@yandex.ru

Abstract. Simulation model of probe routing protocol for use in wireless networks with dynamically changing topology is considered. Principles of simulation model construction in MATLAB software environment are described. The results of network simulation for different variants of protocol parameters are presented. The features of probe routing protocol are investigated. The necessity of the optimal choice of start node for protocol to reduce the algorithm convergence time is shown. The noise immunity of the routing protocol is investigated.

Keywords: routing; protocol; simulation model; wireless networks; MANET.

Введение.

Перспективным подклассом беспроводных телекоммуникационных сетей являются ad hoc сети (MANET – Mobile Ad hoc NETworks) – сети с динамически изменяющейся топологией [1,2]. Каждый узел в ad hoc сети работает одновременно как терминальный узел и как маршрутизатор. Ключевой задачей в ad hoc сетях является задача маршрутизации.

Маршрутизация принадлежит сетевому уровню относительно семиуровневой ISO/OSI модели. Протоколы маршрутизации используются для обеспечения узлов информацией, необходимой для отправки пакетов следующему узлу на пути от источника до получателя по всем маршрутам.

Метод зондовой маршрутизации [3] обеспечивает высокую скорость построения маршрутно-адресных таблиц на узлах в условиях непредсказуемых изменений топологии сети. При этом цикл зондирования обеспечивает построение всех возможных маршрутов движения пакетов с упорядочением по приоритетам. Наивысшим приоритетом обладает маршрут с минимальным временем достижения цели.

Суть метода заключается в следующем: с любого узла сеть зондируется короткими пакетами, называемыми зондами, которые накапливают в себе информацию о состоянии сети. Каждый зонд содержит битовую карту, длина которой равна максимально-возможному числу узлов сети. При прохождении узла в битовой карте зонда устанавливается единица в позиции, определяемой номером узла. При получении зонда узел анализирует информацию, содержащуюся в битовой карте, и по результатам анализа добавляет записи в собственную маршрутно-адресную таблицу. После чего узел проверяет ряд условий для принятия решения о репликации или уничтожении зонда. В случае репликации в зонд добавляется информация о прохождении текущего узла и зонд рассылается по всем исходящим ветвям текущего узла.

Маршрутно-адресные таблицы (матрицы маршрутизации) строятся на каждом узле сети. Число столбцов в матрице равно числу целевых узлов в сети (номер текущего узла из списка целевых узлов исключается, но столбец текущего узла формально присутствует в матрице). Каждый элемент матрицы маршрутизации содержит номер порта текущего узла, указывающего направление, через которое следует передавать пакет для целевого узла. При зондовом протоколе матрица маршрутизации содержит столько строк сколько портов имеет текущий узел. Строки упорядочены по приоритетам. В первой строке содержатся направления высшего приоритета, обеспечивающего наиболее быструю доставку пакета к целевым узлам. Во второй строке содержаться направления, обеспечивающие более медленную доставку пакета по сравнению с первой и т.д., таким образом приоритет направлений снижается при увеличении номера строки матриц маршрутизации. Пример построенной матрицы маршрутизации для узла 5 показан на рис. 1.

	Node-1	Node-2	Node-3	Node-4	Node-5
1	2	3	1	1	-1
2	1	2	4	2	-1
3	4	4	3	3	-1
4	3	1	2	4	-1

Рис. 1. Матрица маршрутизации

В начале цикла маршрутизации маршрутно-адресная таблица узла заполнена нулями за исключением столбца, соответствующего текущему узлу, который заполнен значением (-1). Если зонд прибыл в узел первым, то заполняется первая строка матрицы маршрутизации, следуя правилу: в элементы строки с номерами узлов, через которые прошел зонд, заносится номер порта, через который зонд был получен на текущем узле. Поступление последующих зондов на текущий узел приводит к заполнению нулевых элементов первой строки, которые не были заполнены ранее, а в случае их занятости последовательно заполняются нулевые элементы второй и последующих строк. Если в момент поступления зонда все элементы матрицы маршрутизации узла заполнены, то зонд уничтожается. Зонд будет также уничтожен, если информация на узле уже содержит информацию, доставленную зондом. В остальных случаях зонд добавляет в свою битовую карту текущий узел и реплицируется по всем исходящим направлениям. В случае обнаружения цикла, т.е. когда информация, доставленная зондом уже содержит номер текущего узла зонд рассылается по всем направлениям кроме того по которому он был получен (для стартового узла это ограничение не действует).

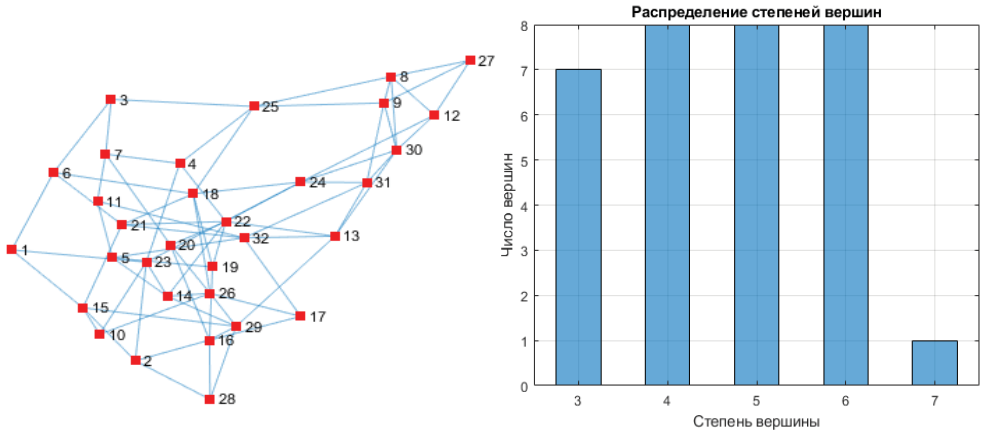
Программная модель

Оценку характеристик протоколов маршрутизации осуществляют как правило методом имитационного моделирования. Для разработки имитатора протокола была выбрана программная среда МАТЛАБ. Создание имитационных моделей протоколов маршрутизации в среде МАТЛАБ может быть основано на принципе

«календаря событий». Календарь представляет собой общую очередь в которой размещаются служебные пакеты, поступающие от всех узлов сети. В протоколе маршрутизации служебные пакеты передаются между смежными узлами. Модельный пакет содержит адресную часть, служебную информацию и метку времени, определяющую время наступления события связанного с началом обработки пакета на целевом узле. Метка времени порождаемого пакета определяется скоростью распространения пакета через сегмент сети, а также меткой времени последнего пакета в очереди на том же сегменте, таким образом моделируются выходные очереди маршрутизаторов. Общая очередь календаря событий обрабатывается во временной шкале по дисциплине «первый пришел-первый обработан».

Результаты моделирования

Моделирование проводилось для сети, состоящей из 32 узлов. Топология сети и распределение степеней связанности вершин показаны на рис. 2.



а) б)

Рис. 2 Топология тестовой сети и распределение степеней связанности вершин

При моделировании предполагалось, что все каналы связи имеют одинаковые задержки. На рис. 3 показана динамика трафика служебных пакетов при скорости в каналах 1200 бит/сек. Размер зонда выбран равным 12 байт. Расчетная пропускная способность данной сети равна 177600 бит/сек. На приведенных графиках единица относительного времени соответствует длительности пересылки зонда по каналу связи. В качестве стартового узла использовался первый узел. В результате моделирования получено:

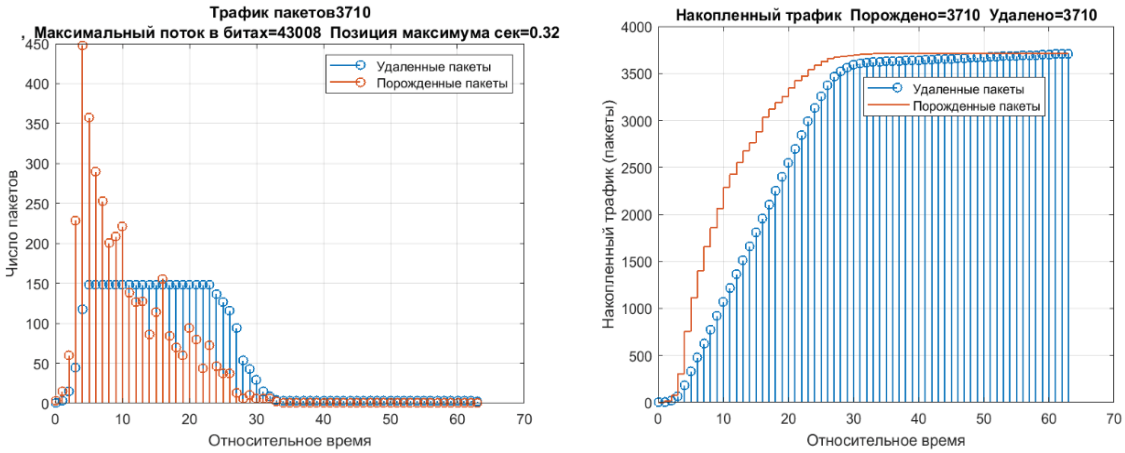
– Полный служебный трафик зондов составил 3710 пакетов, при размере каждого зондового пакета 12 байт.

– Время сходимости алгоритма маршрутизации 5.04 сек при скорости передачи данных 1200 бит/сек.

– Средняя нагрузка на сеть на интервале сходимости 0.398 от пропускной способности сети.

– Пиковая нагрузка на момент максимума трафика равна 1.27 от пропускной способности сети.

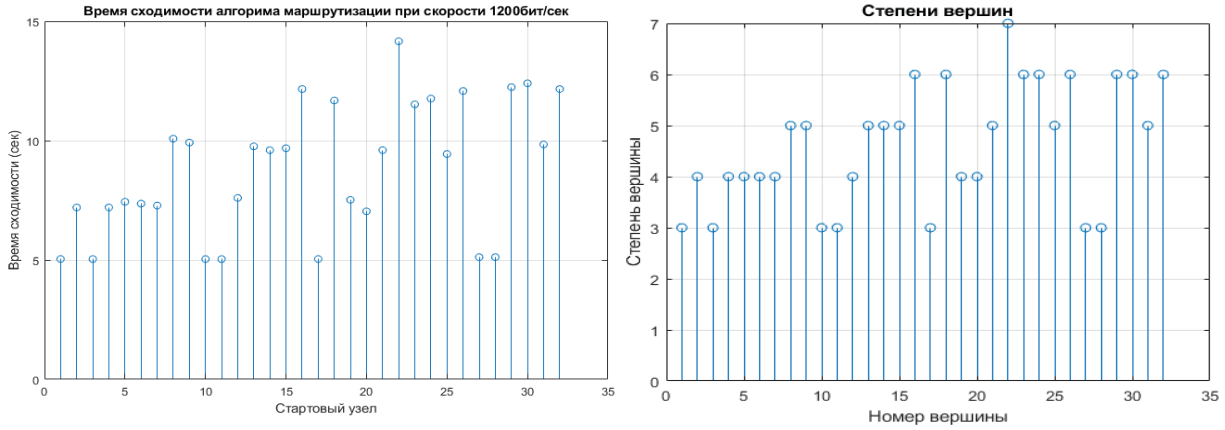
– Поскольку пиковая нагрузка превышает пропускную способность возникают очереди на выходе маршрутизаторов. Максимальная длина выходной очереди при данных условиях эксперимента составила 29 пакетов.



а) Динамика трафика б) Накопленный трафик

Рис. 3 Динамика служебного трафика зондового протокола маршрутизации

Для зондового протокола время сходимости алгоритма маршрутизации и нагрузка сети зависит от стартового узла распространения зондов. На рис. 4а) показана скорость сходимости алгоритма маршрутизации в зависимости от выбора стартового узла.

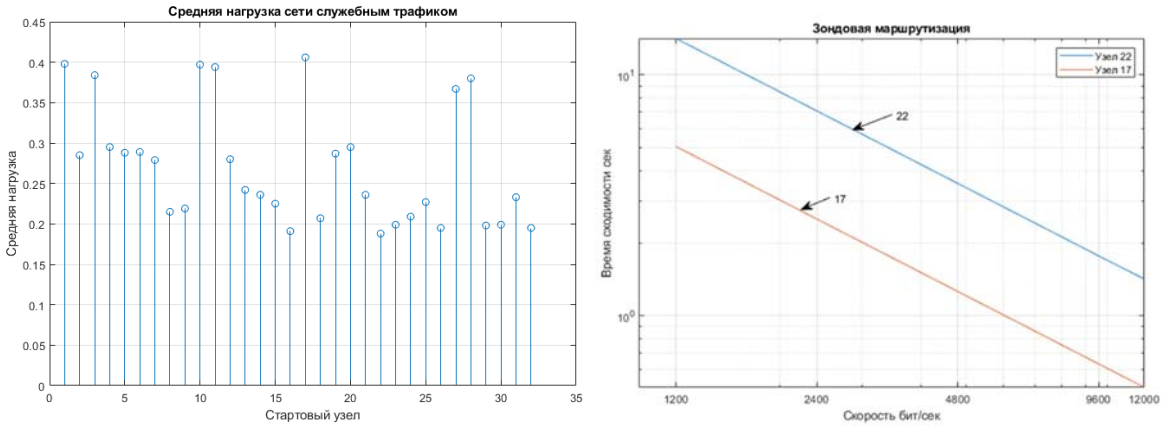


а) б)

Рис. 4. Эффект влияния стартового узла на время сходимости алгоритма

Максимальное время равно 14.16 сек. (узел 22), минимальное время равно 5.04 сек. (узел 17). На рис. 4б) показаны степени вершин исследуемой сети. Сравнение двух графиков показывает, что существует явная зависимость времени сходимости алгоритма от степени стартового узла, чем выше степень стартового узла, тем больше время сходимости алгоритма маршрутизации.

На рис. 5а) представлена зависимость средней нагрузки создаваемой служебным трафиком в зависимости от стартового узла. По оси ординат отложена нагрузка, нормированная к пропускной способности сети. Объем трафика для стартового узла 17 составил 362976 бит (3781 пакет), для стартового узла 22: 472224 бит (4919 пакетов).



а) б)

Рис. 5. Средняя нагрузка на сеть и время сходимости алгоритма зондовой маршрутизации

Максимальная степень загрузки сети служебным трафиком 0.406 (узел 17) а минимальная 0.188 (узел 22). Из приведенных графиков видно, что чем выше степень загрузки сети служебным трафиком, тем меньше время сходимости алгоритма маршрутизации. Учитывая зависимость времени сходимости алгоритма от степени вершины можно заключить что, степень загрузки служебным трафиком тем выше, чем меньше степень стартовой вершины.

С увеличением скорости передачи данных время сходимости алгоритма маршрутизации линейно уменьшается. Характер зависимости для стартовых узлов 17 и 22 показан на рис 5б). На скорости 9600 бит/сек время сходимости для стартового узла 22 составляет 1.77 сек, а для узла 17 составляет 0.63 сек. С увеличением скорости пропускная способность сети линейно увеличивается, при этом нормированная нагрузка сети по служебному трафику не изменяется.

Дефекты матриц маршрутизации

В идеальном варианте работы алгоритма зондовой маршрутизации предполагается, что в процессе распространения зондов по сети все элементы матриц маршрутизации будут полностью заполнены. Так и происходит для сетей с малым количеством узлов. Однако результаты моделирования для тестовой сети с 32

узлами показывают, что по завершению алгоритма маршрутизации полного заполнения матриц не происходит – в матрицах маршрутизации остаются не заполненные элементы (дефекты). Число дефектов в матрицах маршрутизации зависит от стартового узла. На рис. 6 показаны количественные оценки суммарных дефектов матриц маршрутизации в зависимости от стартового узла. При расчете оценок, суммирование дефектов выполнялось по всем узлам и нормировалось в процентах к общему объему заполняемых элементов. Из графика видно, что объем дефектов невелик и в худшем случае не превосходит 0.5%. Сравнение графика оценки со степенями вершин показывает, что минимальный процент дефектов достигается для стартового узла с максимальным числом портов (максимальной степенью вершины). Дефекты в матрицах маршрутизации концентрируется в строках с наименьшим приоритетом направлений. При практической реализации алгоритма маршрутизации не заполненные позиции матриц, могут быть без ущерба заполнены значениями строки с более высоким приоритетом.

Рис. 6. Дефекты в матрицах маршрутизации

Помехоустойчивость алгоритма маршрутизации

При передаче пакетов в реальном радиоканале помехи и замирания сигналов приводят к возникновению битовых ошибок. Для протокола маршрутизации пакетами являются зонды, несущие информацию о маршрутах их распространения по сети. Будем полагать, что ошибка обнаруживается при приеме зонда на входе маршрутизатора (например, по контрольной сумме пакета). Зонд с обнаруженной ошибкой отбрасывается и не участвует далее в процессе формирования маршрутно-адресных таблиц. Характеристикой интенсивности помех при этом допущении может служить вероятность потери пакета. Для топологии тестовой сети (32 узла) генерируемое число зондов в зависимости от стартового узла лежит в диапазоне 3500-4600 и не зависит от скорости передачи данных в канале. Потери зондов может приводить к дополнительным дефектам матриц маршрутизации. При моделировании процесса потери пакетов предлагается в общем потоке генерируемых зондов отбрасывать пакеты с частотой равной вероятности ошибки потери пакета в канале. При этом ошибки пакетов распределяются по каналам следуя логики протокола маршрутизации. Оценку возникающих дефектов матриц маршрутизации выполняется при разных стартовых узлах процедуры маршрутизации и среди них выбирается наихудшая оценка. Базой для сравнения будут дефекты матриц маршрутизации при отсутствии помех. Результаты эксперимента приведены в Таблица 1. На рис. 7 представлен соответствующий график зависимости.

Таблица 1

Зависимость дефектов матриц маршрутизации от вероятности потерь зондов

Вероятность потери зонда	0	0.0001	0.0005	0.001	0.005	0.01
Дефекты матриц маршрутизации (%)	0.479	0.479	0.479	0.479	0.588	0.828

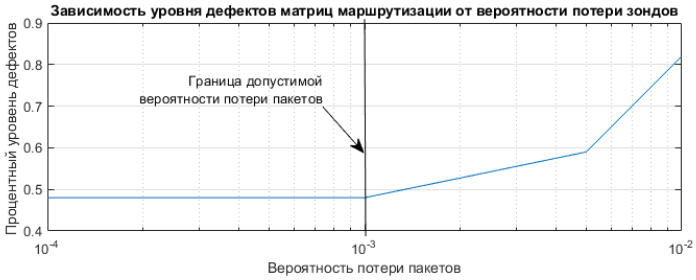


Рис. 7. Зависимость уровня дефектов матриц маршрутизации от вероятности потери зондов

Из представленных результатов следует, что работа протокола маршрутизации не нарушается если вероятность потери пакета не превышает 0.001.

Выводы.

Протокол зондовой маршрутизации является распределенным, работает в асинхронном режиме и обладает исключительно простой алгоритмической реализацией. Благодаря этим особенностям обеспечивается высокая скорость сходимости алгоритма. Причем время сходимости уменьшается пропорционально увеличению скорости передачи данных. Метод зондовой маршрутизации позволяет построить несколько вариантов маршрутов и упорядочить их по предпочтительности. Протокол маршрутизации учитывает фактические задержки в каналах связи и поэтому может адаптироваться к степени загрузки каналов сети. Алгоритм обладает достаточной помехоустойчивостью для работы в радиосетях.

СПИСОК ЛИТЕРАТУРЫ

1. Muthana Najim Abdulleh, Salman Yussof, Hothefa Shaker Jassim Comparative Study of Proactive, Reactive and Geographical MANET Routing Protocols // Communications and Network, 2015, 7, 125-137 Published Online May 2015 in SciRes. http://www.scirp.org/journal/cn http://dx.doi.org/10.4236/cn.2015.72012
2. Wesam Almobaideen, Roba Al-Soub, Azzam Sleit, MSDM: Maximally Spatial Disjoint Multipath Routing Protocol for MANET // Communications and Network, 2013, 5, 316-322 Published Online November 2013 (http://www.scirp.org/journal/cn) http://dx.doi.org/10.4236/cn.2013.54039
3. Аванесов М.Ю. Метод зондового управления потоками данных в мультисервисных сетях с быстро меняющейся структурой // Информация и космос, №3, 2007.- с.35-40.

УДК 681.5 519

ОЦЕНКА ЭФФЕКТИВНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Зубаха Александр Максимович, Подружкина Татьяна Александровна, Саратов Дмитрий Николаевич, Редковников Владислав Александрович
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: iamvladr@gmail.com

Аннотация. В статье описаны подходы к оценке эффективности автоматизированных систем управления, представлены показатели и математические методы их расчета при оценке эффективности АСУ, рассмотрены примеры расчета показателей эффективности АСУ.

Ключевые слова: автоматизированная система управления; показатели эффективности; человеко-машинная система; алгоритм функционирования; вероятность достижения поставленной цели; время достижения поставленной цели; надежность программного обеспечения.

ASSESSMENT OF THE EFFECTIVENESS OF AUTOMATED CONTROL SYSTEMS

Zubaha Aleksandr, Podruzhkina Tatiana, Saratov Dmitriy, Redkovnikov Vladislav
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mail: iamvladr@gmail.com

Abstract. During the implementation and operation of automated control systems (ACS) in various spheres of human activity there is a problem of an estimation of its efficiency. Because ACS, as a rule, complex system, for her comprehensive assessment indicators should be used, which, on the one hand, user-friendly management information system, and on the other hand reflect the effectiveness of its implementation and operation.

Keywords: automated control system; performance indicators; human-machine system; the algorithm of functioning; the probability of achieving the objectives; time to achieve this goal; the reliability of the software.

Введение.

При внедрении и эксплуатации автоматизированных систем управления (АСУ) всегда возникает проблема оценки ее эффективности. АСУ является сложной системой, и для ее всесторонней оценки необходимо использовать показатели, которые, с одной стороны, понятны пользователям АСУ, а с другой стороны, отражают эффективность ее внедрения и эксплуатации.

Автоматизированная система управления (АСУ) это комплекс аппаратных и программных средств, предназначенный для управления различными процессами в рамках технологического процесса, производства, предприятия. Сегодня АСУ применяются в различных сферах человеческой деятельности.

Современные автоматизированные системы строятся, как правило, на основе компьютерных сетей. Компьютерная сеть в совокупности с программным обеспечением и пользователями, по сути, и есть человеко-машинная система, призванная повысить эффективность, прежде всего, управленческой деятельности человека. Поэтому при оценке эффективности АСУ необходимо учитывать такие составляющие управленческого процесса, как надежность и оперативность функционирования системы [1].

В качестве основных показателей эффективности предлагаются следующие показатели:

1. Вероятность достижения поставленной цели - $P_ц$.

2. Время достижения поставленной цели - $M(T_ц)$.

3. Надежность программного обеспечения.

Для оценки вероятности достижения поставленной цели и времени достижения поставленной цели необходимо построить алгоритм функционирования АСУ при выполнении управленческих действий. Алгоритм функционирования удобно представить в виде сетевого графика и поясняющей таблицы [2,3,4].

В сетевом графике и таблице приняты следующие обозначения – таблица 1.

Таблица 1

Обозначения элементов сетевого графика

Обозначение	Назначение
A_{1-3} →	Стрелкой обозначается дуга сетевого графика, обозначающая выполняемую работу между двумя узлами для перехода ЧМС из одного состояния в другое.
a_1	Узел сетевого графика (вершина), обозначающий начальное состояние ЧМС или после выполненной конкретной работы.

Применение сетевого графика иллюстрируется на примере построения упрощенного алгоритма функционирования территориального подразделения МВД [5,6] при поступлении сигнала о происшествии (рис.1).

Таблица 2

Содержание работ

№ п/п	Работа	Содержание работы	Вершина, на которую опирается работа
1.	А1-2	Поступление сигнала.	а1
2.	А2-3	Оценка ситуации.	а2
3.	А3-4	Направление сил и средств.	а3
4.	А4-5	Прибытие сил к месту происшествия.	а4
5.	А5-10	Начало действий.	а5
6.	А5-6	Уточнение обстановки на месте и доклад.	а5
7.	А6-7	Анализ обстановки.	а6
8.	А7-8	Принятие решений о производстве действий.	а7
9.	А8-9	Направление дополнительных сил и средств.	а8
10.	А9-10	Реализация плана действий.	а9
11.	А10-11	Завершение мероприятий.	а10
12.	А11-12	Анализ принятых решений и полученных результатов.	а11
13.	А12-13	Подготовка отчета.	а12

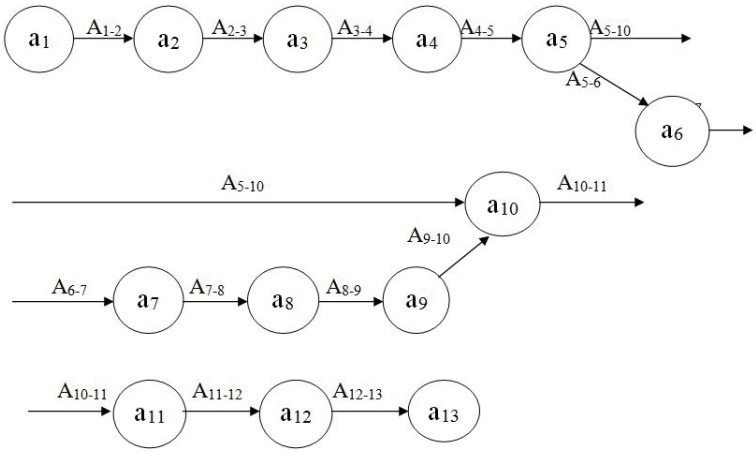


Рис. 1. Алгоритм функционирования

Вероятность достижения поставленной цели - Рц.

По разработанному алгоритму функционирования системы управления проводится большое количество реализаций, и вероятность достижения поставленной цели определяется соотношением – формула (1) [3,6].

$$P_ц = \frac{m}{n}, \quad (1)$$

где n - общее число реализаций алгоритма функционирования;
m - число положительных реализаций алгоритма функционирования.

Реализация алгоритма функционирования считается положительной, если все Ai его работы выполнены и если хотя бы одна работа не выполнена - реализация считается отрицательной.

Вероятность одной Рцi реализации определяется формулой (2):

$$P_{цi} = \prod_{i=1}^{k} P(A_i), \quad (2)$$

где
$P(A_i)$ - вероятность выполнения A_i работы;
i –номер работы;
k –общее количество работ.

При отрицательной реализации алгоритма функционирования вероятность невыполнения Ai работы или выполнения работы с ошибкой – формула (3).

$$P'(A_i) = 1 - P(A_i) \quad (3)$$

Выбор положительной или отрицательной реализации Ai определяется на основании статистических данных работы ЧМС, полученных на этапе эксплуатации системы.

Время достижения поставленной цели - M(Тц).

Время достижения поставленной цели определяется как математическое ожидание времени выполнения одной реализации алгоритма функционирования – формула (4).

$$M(T_ц) = \sum_{i=1}^{m} M(T_i), \quad (4)$$

где $M(T_i)$ - математическое ожидание времени выполнения A_i работы.

В свою очередь

$$M(T_i) = (\sum_{i=1}^{m} T_i) /m, \quad (5)$$

где
m - число положительных реализаций алгоритма функционирования.
T_i – время выполнения i – й работы.

Из приведенных формул видно, что при определении математического ожидания времени выполнения учитываются только положительные реализации алгоритма функционирования.

Если известны надежность и время выполнения работы в условиях отсутствия компьютерной сети, то тогда эффективность внедрения сетей определится с помощью следующих показателей: приращение надежности функционирования ЧМС за счет внедрения сети - ΔРс и приращение оперативности функционирования ЧМС за счет внедрения сети - ΔТс.

$$\Delta P_с = P_ц - P_{бс} \quad (6)$$

$$\Delta T_с = M(T_ц) - M(T_{бс}) \quad (7)$$

3. Надежность программного обеспечения.

Надежность ПО характеризуется его безотказностью и восстанавливаемостью.

Безотказность ПО это свойство сохранять свою работоспособность при использовании его в процессе функционирования ЭВМ.

Безотказность ПО целиком определяется его корректностью, т.е. зависит от наличия ошибок, внесенных в него на этапе создания и эта зависимость, отражающая изменение во времени надежности ПО, имеет вид [3,4], представленный на рис.2

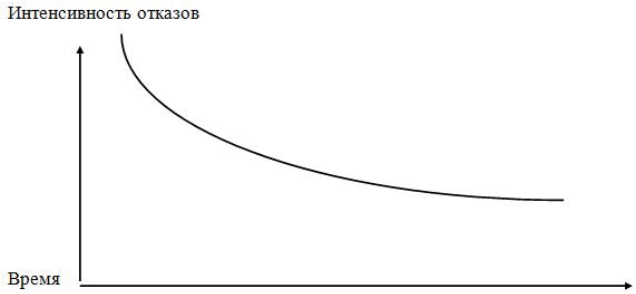


Рис. 2. Интенсивность отказов ПО

Восстанавливаемость ПО определяется затратами времени и труда на устранение отказа, возникшего из-за появившейся программной ошибки и может быть оценена средней продолжительностью устранения ошибки в программе и восстановления ее работоспособности.

Причины отказов ПО:

1. Ошибки, скрытые в самой программе.

В процессе создания программного продукта невозможно обнаружить и ликвидировать все ошибки. Наличие скрытых ошибок - главный фактор нарушения нормальных условий функционирования программного обеспечения. Выделяют следующие классы ошибок в программах:

а). Ошибки вычислений.
б). Логические ошибки.
в). Ошибки ввода-вывода.
г). Ошибки манипулирования данными.
д). Ошибки совместимости.
е). Ошибки сопряжений.

2. Искажение входной информации, подлежащей обработке, возникает, когда входные данные не попадают в область допустимых значений переменных программы. Причинами искажения входной информации являются:

а). Искажение данных на первичных носителях информации.
б). Сбои и отказы в аппаратуре передачи или приема информации.
в). Сбои в канале связи.
г). Ошибки пользователя при подготовке входной информации.

3. Неверные действия оператора.
4. Неисправности аппаратуры.

В зависимости от степени серьезности последствий ошибок в программе может возникнуть полное прекращение выполнения функций на длительное или неопределенное время или краткосрочное нарушение вычислительного процесса. Наиболее типичными признаками появления ошибок в программе являются:

1. Преждевременное (аварийное) окончание выполнения программы.
2. Недопустимое увеличение времени выполнения программы или ее зацикливание.
3. Полная потеря или значительное искажение накопленных данных, необходимых для решаемых задач или искажение отдельных элементов данных в результате обработки искаженной исходной информации.
4. Нарушение последовательности вызова отдельных программ или отдельных модулей программы.

Для оценки надежности ПО используются аналитические модели надежности, которые дают возможность исследовать закономерности появления ошибок в программах, а также прогнозировать надежность ПО при его разработке и эксплуатации. Эти модели строятся на предположении, что появление ошибки является случайным событием и, следовательно, имеет вероятностный характер. Поэтому при построении моделей используются следующие характеристики надежности:

Функция надежности P(t), определяемая как вероятность того, что ошибки программы не проявятся на интервале времени от 0 до t, т.е. время ее безотказной работы будет больше t.

Функция ненадежности Q(t), определяется как вероятность того, что на интервале времени от 0 до t возникнет отказ ПО.

Таким образом, из приведенных определений следует:

$$Q(t) = 1 - P(t) \quad (8)$$

Средняя наработка на отказ T_0 - математическое ожидание временного интервала между последовательными отказами.

Интенсивность отказов $\lambda(t)$ - определяется как среднее число отказов в единицу времени. Интенсивность отказов и функция надежности связаны между собой выражением:

$$P(t) = \exp[-n\lambda(t)dt] \quad (9)$$

Число обнаруженных отказов n - определяется как количество выявленных отказов на интервале тестирования.

Как было сказано выше оценка показателей надежности производится на основе аналитических моделей надежности ПО, которых существует большое множество:

1. Модель надежности программ с дискретно-понижающейся частотой (интенсивностью) появления ошибок.
2. Модель надежности программ с дискретным увеличением времени наработки на отказ.
3. Экспоненциальная модель надежности программ.
4. Модель надежности больших программных комплексов.
5. Большое количество моделей названных по имени их авторов: Джелинского-Моранды, Шика-Уолвертона, Липова и др.

Ниже дана характеристика экспоненциальной модели и модели оценки надежности больших программных комплексов.

Экспоненциальная модель основана на предположении об экспоненциальном характере изменения во времени числа ошибок в программе, и на предположении о том, что интенсивность отказов пропорциональна числу оставшихся ошибок. В качестве показателей надежности ПО в модели используются:

T - среднее время наработки на отказ;

n - число обнаруженных отказов;

$\lambda(\tau)$ - интенсивность отказов.

Пусть

M - число ошибок в программе перед фазой тестирования;

$m(\tau)$ - конечное число исправленных ошибок;

$m_0(\tau)$ - число оставшихся ошибок;

τ - интервал тестирования (время тестирования).

Тогда

$$m_0(\tau) = M - m(\tau) \tag{10}$$

Если исходить из предположения, что в процессе корректировки новые ошибки не появляются, т.е. интенсивность исправления ошибок равна интенсивности их обнаружения, то в этом случае среднее время наработки на отказ (T0) и интенсивность наработки на отказ определяется выражениями:

$$T_0 = T_0' \exp(\lambda(\tau) / MT_0') \tag{11}$$

$$\lambda(\tau) = 1/T_0 \tag{12}$$

где T_0' - исходное значение среднего времени наработки на отказ перед тестированием;

Очевидно, что время наработки на отказ увеличивается по мере выявления и устранения ошибок.

Оценка надежности больших ПК трудоемкий процесс, связанный с большим количеством тестовых прогонов всего комплекса. Показателем надежности больших ПК является вероятность безотказной работы - Рк и определяется она следующим соотношением:

$$P_к = m/n, \tag{13}$$

где

n - общее количество прогонов;

m - количество прогонов с положительным результатом.

Большие программные комплексы, как правило, строятся по модульному принципу, поэтому надежность каждого n-го прогона всего программного комплекса определяется как функция надежности его составных частей.

$$P_{кп} = f(P_{кi}), \tag{14}$$

где

$P_{кп}$ - вероятность безотказной работы всего ПК за один прогон;

$P_{кi}$ - вероятность безотказной работы i-го программного модуля.

При определении Pкп приняты следующие допущения:

1. Надежности модулей ПК величины независимые.

2. Общий результат работы программы будет некорректным, если хотя бы в одном модуле обнаружена в процессе прогона ошибка.

3. Надежность каждого модуля определена.

4. Надежность межмодульного обмена определена.

Функционирование программного комплекса описывается направленным графом состояний (рис.3). На представленном графе каждая вершина, обозначенная кругом, соответствует программному модулю, который имеет определенную надежность ($P_{кi}$), а каждая дуга соответствует направлению передачи управления от модуля к модулю. Передача управления от модуля к модулю также осуществляется с определенной надежностью (P_{ij}).

Таким образом показателями надежности большого ПК при n-м прогоне являются названные выше вероятность безотказной работы всего за один прогон ПК, вероятность безотказной работы i-го программного модуля и P_{ij} - вероятность безотказной передачи управления между модулями.

Если модуль N_i выдает правильный результат, то осуществляется переход к выполнению модуля N_j с вероятностью $P_{кi}P_{ij}$. Переход в состояние C соответствует корректному завершению программы и происходит с вероятностью ($P_{кп}$). Эта вероятность определяется следующим выражением – формула (15):

$$P_{кп} = \prod_{i=1}^{N} P_{кi}P_{ij} \tag{15}$$

При появлении ошибки переход осуществляется в состояние F, что соответствует некорректному выполнению программы независимо от того, как выполнены другие модули ПК и, как следствие, отрицательной реализации прогона в целом.

Пример.

Программный комплекс состоит из семи модулей и его функционирование описывается графом состояний, представленном на рис. 3. Требуется определить:

1. Вероятность безотказной работы ПК за 55 сеансов, из которых три было отрицательных.

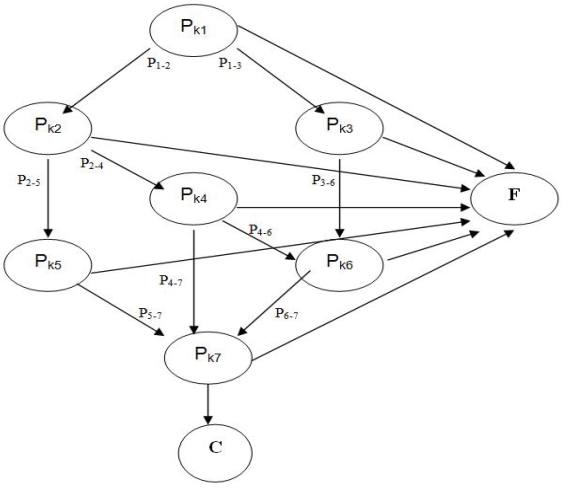


Рис. 3. Граф состояний программного комплекса

2. Вероятность безотказной работы ПК за один прогон, если $P_{к1}$= 0,992, $P_{к2}$= 0,995, $P_{к3}$= 0,989, $P_{к4}$= 0,997, $P_{к5}$= 0,99, $P_{к6}$= 0,987, $P_{к7}$= 0,999, а P_{1-2}= 0,991, P_{1-3}= 0,993, P_{2-4}= 0,998, P_{2-5}= 0,989, P_{3-6}= 0,996, P_{4-6}= 0,997, P_{4-7}= 0,995, P_{5-7}= 0,988, P_{6-7}= 0,993, P_{7-c}= 1.

1. $P_к$ = 52/55 = 0,945

2. $P_{кп}$ = (0,992∗0,991)∗(0,992∗0,993)∗(0,995∗0,998)∗(0,995∗0,989)∗(0,989*0,996)∗
*(0,997∗0,997)∗(0,997∗0,995)∗(0,99∗0,988)∗(0,987∗0,993)∗0,999 = 0,88

Заключение.

Таким образом, рассмотрены и описаны подходы к оценке эффективности автоматизированных систем управления, представлены показатели и математические методы их расчета при оценке эффективности АСУ, рассмотрены примеры расчета показателей эффективности АСУ.

СПИСОК ЛИТЕРАТУРЫ:

1. Давыдов А.В., Куклин В.В., Хайдаров К.А. Информационные сети и телекоммуникационные каналы. URL: http://bourabai.kz/telecom/index.htm.
2. Балдин К.В., Воробьев С.Н., Уткин В.Б. Управленческие решения: учеб. 5-е изд. М.: Изд-ко-торговая корпорация «Дашков и Ко», 2008. 496 с.
3. Шпак В.Ф. Основы автоматизации управления. Петродворец: Военно-морской институт радиоэлектроники Им. А.С. Попова, 1998. Ч. 1. С. 174-181.
4. Автоматизация управления и связь в ВМФ/Н.Ф. Директоров [и др.]. СПб.: Элмор, 2001. С. 176-179.
5. Голубков Е.П. Технология принятия управленческих решений. М.: Дело и сервис, 2005.
6. Вентцель Е.С. Исследование операций. М.: Высш. шк., 2007.

УДК 004.056.53

КРИТЕРИИ И МЕТОДЫ ОЦЕНКИ КАЧЕСТВА ДЛЯ ОБОСНОВАНИЯ ВЫБОРА МЕЖСЕТЕВЫХ ЭКРАНОВ

Протас Роман Сергеевич, Закороев Расул Романович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mails: roprotas@yandex.ru, zakoroev05@mail.ru

Аннотация. Для защиты компьютера и информации, которая хранится на нем используются соответствующие средства информационной безопасности из реестра сертифицированных средств защиты информации ФСТЭК, который включает более 170 межсетевых экранов. Для обоснованного выбора наиболее предпочтительного варианта межсетевого экрана предложено их ранжировать с использованием гармонического алгоритма агрегирования частных показателей качества.

Ключевые слова: угроза; межсетевой экран; безопасность; ранжирование; оптимальный выбор.

CRITERIA AND METHODS OF ASSESSMENT OF QUALITY FOR JUSTIFICATION OF THE CHOICE OF FIREWALLS

Protas Roman, Zakoroev Rasul
St. Petersburg State Marine Technical University
3 Lotsmanskaya Str., St. Petersburg, 190121, Russia
e-mails: roprotas@yandex.ru, zakoroev05@mail.ru

Abstract. For protection of the computer and information, which is stored on it, appropriate means of information security from the register of the certified means of information protection of FSTEC, which turns on more than 170 firewalls are used. For the reasonable choice of the most preferable version of the firewall it is offered to range them with use of a harmonious algorithm of aggregation of private indicators of quality.

Keywords: threat; firewall; security; ranking; optimal choice.

Актуальность.

Файрвол, брандмауэр или межсетевой экран – это одно из самых распространенных средств защиты информации в виде программного или программно-аппаратного комплекса, реализующего функцию защитного барьера между компьютером и сетью, которую можно представить в виде последовательности фильтров. Фильтрация трафика осуществляется на основе набора предварительно сконфигурированных правил, которые называются ruleset.

Каждый из фильтров предназначен для интерпретации отдельного правила. Последовательность правил в наборе существенно влияет на производительность файрвола. Многие файрволы последовательно сравнивают трафик с правилами до тех пор, пока не будет найдено соответствие. Для таких межсетевых экранов правила, которые соответствуют наибольшему количеству трафика, следует располагать как можно выше в списке, увеличивая тем самым производительность [1].

Существует два принципа обработки поступающего трафика. Первый принцип гласит: «Что явно не запрещено, то разрешено». В данном случае, если межсетевой экран получил пакет, не соответствующий ни одному правилу, то он передаётся далее. Противоположный принцип «Что явно не разрешено, то запрещено» гарантирует большую защищённость, так как он запрещает весь трафик, который явно не разрешён правилами. Однако, этот принцип приводит к дополнительной «нагрузке» на администратора. Но самой сложной «нагрузкой» для администратора остается традиционная задача обоснованного выбора лучшего из более, чем 100 возможных вариантов межсетевого экрана.

Для обоснованного выбора необходимо с учетом свойств альтернативных объектов сравнения, порядка и правил их использования обосновать критерии выбора, для чего выполнен следующий анализ.

1. Соединение хотя бы двух компьютеров, позволяющее осуществлять передачу данных между ними, уже является сетью. Даже если пользователи допускают, что они «не интересны» злоумышленникам, их компьютеры после подключения к сети автоматически становятся потенциальной целью для них.

Для того, чтобы совершить «информационное преступление (инцидент, конфликт)» в интернете достаточно получить доступ к любому незащищенному компьютеру. Приложения, созданные злоумышленниками, способны проникнуть по сети на незащищенный компьютер и запускаться незаметно для пользователя. При этом, они могут:

– собирать и пересылать вашу персональную информацию своим создателям или просто удалять, или архивировать важные данные;
– использовать зараженный компьютер для совершения других противоправных действий: рассылки спама, взлома удаленных сервисов и т.д.;
– генерировать большое количество паразитного трафика и делать звонки на платные телефонные номера через модем;
– перенаправлять интернет-браузер на рекламные страницы;
– применять «Фишинг» для финансовых махинаций или кражи персональных данных;
– нарушать работу ПО, установленного на компьютере или ОС в целом.

Злоумышленники используют специальное программное обеспечение для сканирования глобальной сети и поиска незащищенных компьютеров. Такие программы направляют пакет данных каждому компьютеру. Если компьютер не защищен, то он автоматически отвечает на принятое сообщение, и это означает, что система не защищена и может быть атакована. Файрвол предназначен для распознавания таких сообщений и защиты компьютера от атаки. Таким образом, злоумышленники даже не могут узнать, что ваш компьютер подключен к сети.

2. Недостатки межсетевых экранов. К сожалению, межсетевой экран - не решает задачу защиты информации в полном объеме. Брандмауэр фильтрует только тот трафик, который он способен обрабатывать. Существуют протоколы, которые используют алгоритмы шифрования данных (криптографические алгоритмы), из-за чего трафик не может быть интерпретирован. Такая же проблема связанна с туннелированным трафиком: брандмауэр не эффективен, если ему не знаком механизм туннелирования трафика. Для этих случаев необходимы правила, которые будут определять, что делать с таким и подобными трафиками.

3. Выбор межсетевого экрана. В последних редакциях Реестра сертифицированных средств защиты информации ФСТЭК приведены 109 межсетевых экранов [2]. В связи с этим пользователь сталкивается с проблемой выбора. Для того, чтобы осуществить выбор между большим количеством брандмауэров необходимо их ранжировать. Наиболее совершенным в этом аспекте, как известно, является гармонический алгоритм, обладающий минимальной погрешностью агрегирования частных показателей качества.

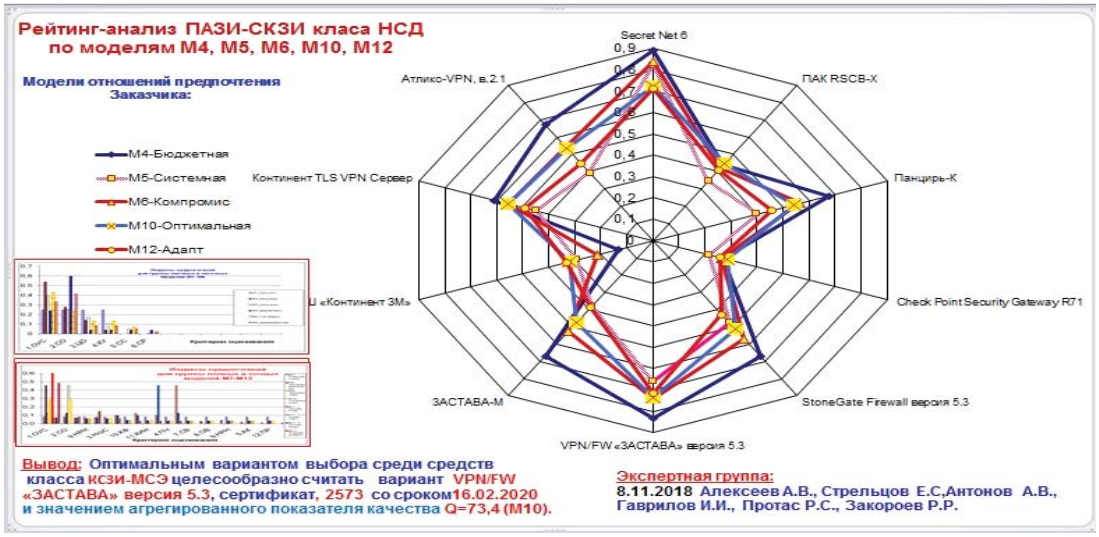


Рис.1. Предварительные результаты ранжирования сертифицированных средств защиты информации в классе «Межсетевые экраны»

Для обоснования выбора и ранжирования по качеству межсетевых экранов предложена следующая система критериев оценки качества:

А. Агрегированный показатель качества (АПК) межсетевых экранов (по гармоническому алгоритму агрегирования групповых и частных показателей качества).

Б. Групповые показатели качества, характеризующие их свойства:

– обобщенный уровень качества по данным сертификации, срок действия сертификата;
– функциональная полнота решения комплекса задач;
– функциональное качество решения комплекса задач;
– возможность информационно-технического сопряжения с другими программно-аппаратными средствами, используемыми в используемой сети;
– стоимость владения, включая стоимость приобретения, расходных материалов, техническую поддержку и т.п.;
– репутационный индекс (по отзывам пользователей) при соответствующих доверительных интервалах;
– сервисные преимущества, включая условия технической поддержки от производителя.

В. Частные показатели качества:

– число портов и типы используемых аппаратных средств;
– пропускная способность;
– энергопотребление;
– срок эксплуатации;
– время отработки заявок по технической поддержке;
– другие, включая неучтенные, критерии и показатели качества.

С использованием данной системы критериев сформирована база данных и знаний по классу сертифицированных средств защиты информации «Межсетевые экраны» и выполнены оценочные расчеты по критерию АПК по методике [3]. Это позволило выполнить их ранжирование по качеству и определить наиболее предпочтительные варианты выбора. На рис. приведены соответствующие результаты.

Ранжирование выполнено по ряду моделей критериальных предпочтений, что позволило реализовать принцип полимодельного подхода к выбору оптимального варианта.

В настоящее время производятся верификация полученных оценок и апробация сформулированных результатов ранжирования.

Выводы.

При использовании сертифицированных средств защиты информации, в том числе класса «Межсетевые экраны» одной из традиционно сложных и проблематичных задач является обоснованный выбор предпочтительных и оптимального варианта из них.

Для обоснованного их выбора с целью получения максимального качества их использования и эффективности эксплуатации с учетом заданных пользователями требований необходимо их ранжирование по агрегированному показателю качества по соответствующей системе критериев и гармоническому алгоритму агрегирования частных и групповых показателей качества.

СПИСОК ЛИТЕРАТУРЫ

1. Электронный ресурс: https://ru.wikipedia.org/wiki/межсетевой_экран (Дата обращения 15.11.2018).
2. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00.
3. Алексеев А.В. Сертификация систем обработки информации: учеб. пособие – СПб: Издательский центр СПбГМТУ, 2010. – 159 с.

УДК 504.064.2.001.18

АВТОМАТИЧЕСКИЙ РАЗЛИЧИТЕЛЬ ВЕТРОВОГО СЛИКА И НЕФТЯНОГО ПЯТНА

Чернецова Елена Анатольевна, Шишкин Анатолий Дмитриевич
Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mails: chernetsova@list.ru, an.dm.shishkin@mail.ru

Аннотация. В статье рассматривается проблема классификации аномалий на морской поверхности на примере радиолокационных изображений нефтяного пятна и ветрового слика. В качестве признаков объектов рассматриваются ряды параметров распределений, аппроксимирующих гистограммы изображений и ряды интенсивности пикселей изображений. Рассмотрен последовательный алгоритм классификации для определения необходимого количества образцов объектов в банке данных.

Ключевые слова: морские аномалии; радиолокационные изображения; классификация объектов; решающее правило; охрана окружающей среды; непараметрический алгоритм

AUTOMATIC DEFINITION OF WIND SLIC AND PETROLEUM SPOT

Chernetsova Elena, Shishkin Anatoly
Russian State Hydrometeorology University
79 Voronejskaja Str., St. Petersburg, 192007, Russia
e-mails: chernetsova@list.ru, an.dm.shishkin@mail.ru

Abstract. The article deals with the problem of classification of anomalies in the sea surface by the example of radar images of oil spills and wind slicks. As the attributes of the objects the ranks of the distribution parameters, approximating the histogram of images and rows of pixel intensity images are considered. The sequence of the classification algorithm is examined to determine the required number of samples of objects in a database.

Keywords: marine anomalies; radar images; classification of objects; the decision rule; environmental protection; nonparametric algorithm

Введение.

При дистанционном зондировании морских акваторий данные представляют собой монохромные радиолокационные изображения (РЛИ), которые используются для обнаружения и классификации выделенных аномалий. Эти данные отправляются на хранение в банк данных, либо претерпевают в системе некоторую обработку и затем передаются потребителю в виде, удобным для принятия решений. Решение задачи классификации базируется на современных алгоритмах, вычислительных и программных средствах.

Для автоматизации решения задачи распознавания нефтяного пятна на морской поверхности, и отличения его от ветрового слика необходимо иметь банк данных РЛИ, по которым производится оценка их параметров.

В работе [2] обсуждалось применение для целей распознавания образов нефтяного пятна и ветрового слика построенных гистограмм оттенков серого цвета на выделенном фрагменте РЛИ. Считаем, что на РЛИ проведена фрагментация выделенных участков и построены гистограммы распределений яркости. В дальнейшем предполагалась аппроксимация этих гистограмм законами распределения вероятностей с определением параметров этих распределений. Однако исследования показали, что, поскольку изображения являются двумерными, законы распределения вероятностей интенсивности пикселей на изображениях нефтяного пятна и ветрового слика могут, как отличаться друг от друга по параметрам, так и быть похожими друг на друга. Поскольку реальные ПРВ не известны, то представляется наиболее целесообразным создание непараметрического автоматизированного классификатора рассматриваемых образов.

Теоретический анализ. Задача исследования состоит в определении минимального количества изображений каждого объекта (нефтяного пятна или ветрового слика), достаточного для работы автоматизированного классификатора объектов, если для работы классификатора используются: а) ряды параметров распределений, аппроксимирующих гистограммы изображений; б) ряды интенсивности пикселей изображений.

В задачах непараметрического оценивания часто делается предположение альтернатив Лемана. В данном исследовании применяется оценка Ходжеса-Лемана, относительно которой было установлено, что она мало отличается от широко распространенной для решения подобных задач статистики Вилкоксона, но уменьшает количество необходимых вычислительных затрат [3].

Оценка сдвига распределений Ходжеса-Лемана. представляет собой медиану всех возможных пар разностей элементов одной и другой групп:

$$r_{ij} = med(x_{ui} - x_{vj}); \; u = 1,..n_i; \; v = 1,..n_j. \qquad (1)$$

где x_{ui} и x_{vj} - параметры пикселей по координате i и j.

Положительное свойство этой медианы состоит в том, что насколько первая группа "больше" второй, настолько вторая "меньше" первой, то есть: rij = -rij. Существенным недостатком медианы Ходжеса-Лемана является нетранзитивность. Если x больше y на a, а s больше y на b, то желательно, чтобы s было больше x на величину $a+b$. Медиана этим свойством не обладает [4].

Однако, поскольку в нашем случае имеется только две альтернативы, то статистику Ходжеса-Лемана использовать правомерно.

В качестве инструмента используем последовательный критерий отношения вероятностей Вальда (п. к. о. в.) [5,6], основанный на последовательных рангах, расставив замеры сравниваемых выборок так, чтобы они чередовались: $x_1, y_1, x_2, y_2, \ldots, x_n, y_n$. Обозначим объединенные замеры на k-том шаге вектором $V(k)=[v_1, v_2, \ldots, v_k]$, где $v_1 = x_1, v_2 = y_1$ и т.д. Пусть $S(k)=[S_1, S_2, \ldots, S_k]$ есть вектор последовательных рангов для $V(k)$, а

$$\lambda_k = \frac{P_k(S(k)/H_1)}{P_k(S(k)/H_0)} \tag{2}$$

представляет собой последовательное отношение вероятностей на k-том шаге процесса [6]. Если верна гипотеза H_0, то для произвольного вектора S из $S(k)$ имеем $P_k(S(k)=S/H_0)=1/k!$ и, следовательно, можно вычислить $P_k(S(k)=S/H_1)$, учитывая, что каждый полученный вектор S соответствует взаимно однозначным образом определенному порядку объединенных замеров x_i и y_i.

Таким образом, достаточно вычислить

$$P(v_1 \le v_2 \le \ldots \le v_k / H_1) = \int\limits_{-\infty<t_1\le t_2\le\ldots\le t_k<\infty} \ldots \int \prod_{t=1}^{k} df_i(P(t_i)), \tag{3}$$

где $f_i(P(t_i))=P(t_i)$, когда v_i есть x и $f_i(P(t_i))=f(P(t_i))$, когда v_i есть y.

В случае альтернатив Лемана имеем две гипотезы.

Гипотеза о наличии на изображении образа нефтяного пятна $H_0 : G=P(X)$,

против гипотезы о наличии на изображении ветрового слика $H_1 : G=f(P(X))=P^r(X); r>0$.

При этом последовательное отношение вероятностей на k-том шаге

$$\lambda_k = \frac{P_k(S(k)/H_1)}{P_k(S(k)/H_0)} = \frac{k!\,r^{k/2}}{\prod_{i=1}^{k}(\sum_{j=1}^{i} A_j)} \text{ для четных значений } k \tag{4}$$

и

$$\lambda_k = \frac{P_k(S(k)/H_1)}{P_k(S(k)/H_0)} = \frac{k!\,r^{(k-1)/2}}{\prod_{i=1}^{k}(\sum_{j=1}^{i} A_j)} \text{ для нечетных значений } k \tag{5}$$

где $A_j = \begin{cases} 1; & \textit{если} \quad v_j \quad \textit{есть} \quad x, \\ r; & \textit{если} \quad v_j \quad \textit{есть} \quad y. \end{cases}$ (6)

Таким образом, непараметрическая процедура определения количества изображений в банке данных, необходимого для распознавания образов нефтяного пятна или ветрового слика с использованием последовательного критерия отношения вероятностей Вальда сводится к следующим шагам:

Шаг 1: получение последовательного ранга $(k+1)$-й выборки параметра классификации.

Шаг 2: Образовать вектор $A(k+1)$ из $A(k)$ и S_{k+1}…

Шаг 3. Вычислить последовательное отношение вероятностей по формуле (4) или (5) и сравнить с останавливающими границами.

Обозначим e_{ij} - вероятность принятия гипотезы H_i, тогда как в действительности верна гипотеза H_j; $i, j = 0,1$. Тогда останавливающие границы (пороги) в п.к.о.в. Вальда приближенно равны

$$A = \frac{1 - e_{01}}{e_{10}}, \qquad B = \frac{e_{01}}{1 - e_{10}} \tag{7}$$

А связь между средним числом измерений $E(k)$ и параметром r приближенно описывается зависимостью

$$E_r(k) \cong \frac{\log[(1 - e_{10})/e_{01}]}{\log\frac{1}{2}(r^{-1/2} + r^{1/2})}, \tag{8}$$

Для решения рассматриваемой задачи примем $e_{10} = e_{01} = 0{,}1$.

Тогда пороги п.к.о.в. Вальда будут равны A=9,0 и B=0,11.

Компьютерное моделирование непараметрической процедуры п.к.о.в. Вальда. С целью проверки выдвинутых предположений был выполнен компьютерный эксперимент по моделированию описанного выше пошагового последовательного алгоритма. Определялось необходимое количество образцов РЛИ при двух видах исходных параметров: а) по параметрам аппроксимирующих распределений; б) по интенсивности пикселей изображений по вертикали и горизонтали. Результаты компьютерного моделирования непараметрической процедуры п.к.о.в. Вальда приведены в таблице 1.

Таблица 1

Результаты компьютерного моделирования п.к.о.в. Вальда для определения объема банка данных, необходимого для работы автоматического классификатора образов нефтяного пятна и ветрового слика на изображении морской поверхности

Параметр классификации	Необходимое количество изображений, которое должно содержаться в банке данных
Параметры плотностей распределения вероятностей интенсивности пикселей изображения (различие по критерию χ^2 образцового и оцениваемого распределения <5%)	40
Интенсивность пикселей изображения, обрабатываемого по горизонтали	16
Интенсивность пикселей изображения, обрабатываемого по вертикали	15

Выводы.

Моделирование показало, что использование для работы автоматического классификатора образов нефтяного пятна и ветрового слика на изображении морской поверхности в качестве параметра интенсивности пикселей позволит снизить требования к объему банка данных по сравнению с использованием для той же целей аппроксимации гистограмм оттенков серого известными законами распределения вероятностей.

СПИСОК ЛИТЕРАТУРЫ

1. Del Frate et al.: Neural Networks for Oil Spill Detection Using ERS-SAR Data // IEEE Transactions on Geoscience and Remote Sensing, vol.38, NO 5, September 2000, pp.2282-2287
2. Чернецова Е.А. Дистанционный мониторинг нефтяных загрязнений в водной среде. Монография. - Lap Lambert Academic Publishing GmbH&Co.KG , 2011, - 123 p.
3. Роенко А.А., Лукин В.В., Зеленский А.А. Определение параметра сдвига выборки данных с симметричным негауссовым распределением на основе использования методов адаптивного робастного оценивания/Радіоелектронні і комп'ютерні системи, 2005, № 2(10), с.78-87
4. Шеломовский В.В. Электронный учебник по дисциплине «Математическая статистика»/ Мурманский федеральный государственный педагогический университет – [Электронный ресурс] – Режим доступа: http://www.exponenta.ru/educat/systemat/shelomovsky/lab/lab07.asp
5. Шишкин А.Д., Чернецова Е.А. Последовательное решающее правило классификации аномалий на морской поверхности/ Журнал «Системы управления и информационные технологии», №2(52), 2013. – с. 94-97
6. Фу К. Последовательные методы в распознавания образов и обучении машин. / Пер. с англ.-Изд. «Наука».-М.:1971.-256 с.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056

КИБЕРБЕЗОПАСНОСТЬ ЦИФРОВОГО ПРОИЗВОДСТВА И ЭКОНОМИКИ

Зегжда Петр Дмитриевич
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mail: kafedra@ibks.spbstu.ru

Аннотация. В статье проанализированы задачи обеспечения кибербезопасности в эпоху цифровизации. Раскрыты проблемы и задачи поддержания киберустойчивости крупномасштабных цифровых систем ответственного назначения в условиях воздействия новых классов компьютерных атак.

Ключевые слова: безопасность; киберустойчивость; межмашинные сети; управление; цифровизация; АСУ ТП; MANET; IIoT; VANET.

CYBERSECURITY OF DIGITAL INDUSTY AND ECONOMY

Zegzhda Peter
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya Str., St. Petersburg, 195251, Russia
e-mail: kafedra@ibks.spbstu.ru

Abstract. The paper reviews challenges of ensuring cybersecurity in the era of digitalization. The isssues and tasks relative to the cybersustainability of large-scale smart infrastructures under the influence of new classes of cyberthreats are discussed.

Keywords: security; cyber sustainability; machine-to-machine networks; mainanence; digitalization; industrial control system; MANET; IIoT; VANET.

Эволюция передовых производственных систем и Цифровая революция.

В настоящее время развитие постиндустриального общества характеризуется перманентной информационной революцией, состоящей в интеграции Internet-технологий практически со всеми системами АСУ как промышленности, трансопрта и энергетики, так и связи, банковских систем и систем оборонного значения. Более того, информатизация охватила сферу энергетических производств, сделав элементы автоматических систем управления технологическими процессами (АСУ ТП) частью общего киберпространства.

Современная эпоха может быть названа интернетизацией общества. Интернет выступает как универсальная среда, позволяющая с помощью открытых протоколов передачи данных и управления транзитивно замкнуть все информационные аспекты экономики и социальной жизни в единое цифровой пространство – киберпространство. Элементы киберпространства содержат не только данные, но и системы их передачи, обработки и хранения, системы управления этими процессами и реакции, средства защиты, а также их динамически изменяющиеся взаимосвязи, вместе составляющие определенную ценность.

Сегменты киберпространства нового поколения:

- корпоративные и банковские сети;
- мобильные системы и самоорганизующиеся сети;
- облачные сервисы и суперкомпьютеры;
- автоматизированные банковские системы;
- прочая цифровая инфраструктура («умные дома», социальные сети и т.д.).

При этом происходит так называемая четвертая промышленная революция [1], характеризуемая широким применением новых информационных технологий, таких как M2M-сети, IoT, беспилотный транспорт, роботы, технологии искусственного интеллекта. В качестве технологической основы Индустрии 4.0 и передовых промывшленных решений можно привести киберфизические преобразования энергии и ресурсов в сочетании с цифровым управлением, новые технологии обработки данных, аналитические решения и достижения в облатси искусственного интеллекта, развитие человеко-машинных интерфейсов [2] (рис. 1). При этом не является принципиально важным, что выступает в качестве конечной стадии производства, то есть является итоговым продуктом: машины, механизмы, бытовые изделия, интеллектуальные системы, электрическая или тепловая энергия, гидроэнергия и т.д. (рис. 2).

На основании понятия киберпространства, определим кибербезопасность как комплекс мер, направленных на достижение гарантированного состояния независимости киберпространства от ущерба вследствие нарушений в его функционировании.

Понятия киберфизических объектов и систем связаны с трансформацией управления физическими процессами в цифровую сферу. Формальные понятия киберфизических объектов и систем приведены в [3]. Киберфизической объект (КФО) – концептуальная парадигма представления производственных, технологических схем в виде конгломерата средств преобразования различных видов материи и энергии и информационно-телекоммуникационной среды, обеспечивающей как обмен информацией между компонентами, так и устойчивое функционирование всей системы

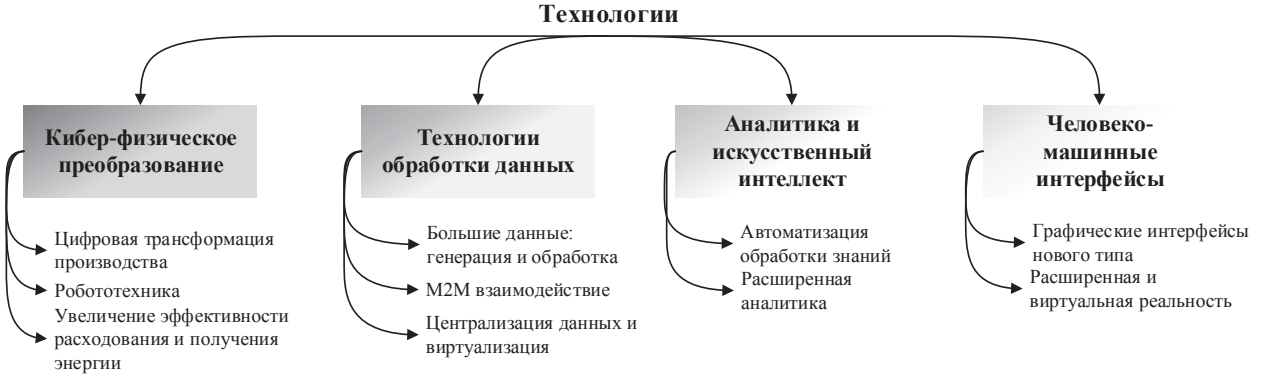


Рис. 1. Технологии четвертой промышленной революции

Угрозы кибербезопасности.

Спектр компьютерных угроз в связи с цифровой трансформацией расширяется до киберугроз, целью которых является не только хищение или уничтожение данных, но и перехват управления системами, инфраструктурой, различными исполнительными механизмами и автоматизированными системами, навязывание своих алгоритмов управления транспортом, энергопроизводством, банками, сервисами, приложениями, инфраструктурой. При этом наблюдаемое в последнее время противостояние в информационно-коммуникационной сфере приняло совершенно новую форму активного взаимного воздействия, следующего игровому сценарию, когда обе стороны целенаправленно реализуют угрозы, направленные на информационные системы противоположной стороны, и стремятся подавить чужие средства безопасности.

Каждый год возникают новые сообщения о громких инцидентах, связанных с различными секторами промышленности и роботизации, при том что пребывание злоумышленников в критических системах обнаруживается далеко не сразу. Срок обнаружения может достигать нескольких лет (зафиксирован рекорд в семь лет пребывания злоумышленников необнаруженными в системе). Мишенью являются как производственные системы, так и поставщики промышленного оборудования. Их продукция используется для экономического шпионажа и разведки.

Необходимо сказать, что из общего числа выявленных инцидентов, более половины занимают направленные атаки (APT) и действия квалифицированных злоумышленников. Лидирует в количестве инцидентов энергетический сектор, за ним следуют критически важные инфраструктуры и беспилотный транспорт [4]. Вектор атаки большинства произошедших инцидентов информационной безопасности в критически важных объектах неизвестен – то есть, организация подтверждала инцидент, однако данные расследования не указывали на метод, используемый для проникновения, в силу необходимости сохранения репутации или отсутствия обнаружения и мониторинга в скомпрометированной сети.

Моделирование критически важных киберфизических систем при управлении безопасностью.

Для решения этой проблемы предлагается операционная модель атаки на цифровые киберфизические системы (КФС). Особенностью данного подхода является упор на описание не всего многообразия атак по цели воздействия, а операций, которые производятся при реализации атаки. Для этого система представляется моделью со счетным числом возможных типов воздействий. В сфере информационной безопасности широко применяются графовые модели [5] описания систем и воздействий на них, в которых все операции можно свести к конечному числу возможных типов операций на графе.

Определим следующие общие требования к модели киберфизической системы:

1. Концептуальная схема модели должна быть адекватна для моделирования сетеподобных объектов и их взаимодействий.

2. Выбор отдельных элементов сети может варьироваться без существенного изменения вида модели и с сохранением основных подходов к моделированию.

3. Определение функционала системы должно складываться из декомпозируемых функций. Можно выделить следующие группы функций:

– функции обработки информации (преобразование, хранение, передача);

– функции обеспечения безопасности (управление доступом, антивирусные действия, фильтрация, криптографические преобразования, аутентификация, управление полномочиями);

– функции мониторинга и сбора данных.

4. Система должна включать компонент, отвечающий за оценку устойчивости и применение механизмов управления.

Для описания таких систем графовые модели обладают рядом преимуществ:

Универсальность: любая КФС может быть представлена как граф, вершины которого хосты КФС, а рёбра характеризуют их взаимодействие;

Полнота моделирования: любое деструктивное воздействие, независимо от его источника, отразится либо в нарушении количества и параметров узлов, либо в нарушении количества и параметров связей.

Иерархичность: при необходимости, модель может быть детализирована с помощью представления любого хоста в виде графа, состоящего из других хостов.

При этом нарушение, независимо от его источника, может быть выражено одним из следующих случаев:

– изменение числа вершин графа;
– изменение числа ребер графа;
– изменение параметров вершин графа;
– изменение параметров ребер графа.

Таким образом, для моделирования КФС может быть использован иерархический граф, который на уровне устройств может быть представлен как граф $G=(V,E)$, где V – непустое множество вершин, представляющих собой на верхнем уровне системы взаимодействующие устройства, а E – множество ребер, представляющих собой связи между вершинами. Каждая вершина графа G при этом может быть представлена на втором уровне описания системы как граф $G'=(V',E')$, где V' – непустое множество вершин, представляющих собой взаимодействующие модули, а E – множество ребер, представляющих собой связи между ними. Декомпозиция возможна до уровня отдельных модулей, каждый из которых способен выполнять крайней мере одну функцию (любого уровня декомпозиции функций), принимать и передавать сообщения одного из заданных типов от других модулей.

Каждая вершина графа (на верхнем уровне - хост) $v_i \in V$ обладает множеством функций $F=F_r \cup F_p$ и множеством параметров P_V, где F_r – множество функций, которые хост выполняет в данном киберфизическом процессе, а F_p – множество функций, которые хост может выполнять, но не выполняет в данном киберфизическом процессе. Каждая функция $f \in F$ также обладает набором входных и выходных параметров $P=P^{in} \cup P^{out} \mid P^{in}=\bigcup_{i=1}^{|F|} P_i^{in},\ P^{out}=\bigcup_{i=1}^{|F|} P_i^{out} \quad \forall f_i \in F$, связанных с ее полезной деятельностью: $f_i(P_i^{in})=P_i^{out}$. Таким образом, выделяются две группы параметров:

Параметры устройств (на нижнем уровне - модулей) – PV;

Параметры исполняемых функций (входные и выходные) – P.

Каждое ребро $e_i \in E$ обладает единственной функцией – функцией обеспечения коммуникации между соседними вершинами и обладает множеством параметров P_E. Таким образом, множество ребер задает набор бинарных отношений между вершинами.

Каждый физический процесс, выполняющийся в системе, в такой модели состоит из упорядоченного набора функций $\Phi=\{\varphi_1,\ldots,\varphi_m\}$ выполняемых в системе над входными данными и внешними системами («реальными» системами управляющими физическим процессом). Для описания выполнения процесса в киберфизической системе задается отображение Fprocess:Φ→F, где F-функции вершин системы.

В соответствии с введенными обозначениями, так как $F_{process}(\phi_k)=f_i$, а $f_i \in v_j.F$, где $v_j \in V$, киберфизический процесс представляет собой набор путей S на множестве маршрутов графа G, составленных из определенной последовательности функций $s_i \in S : s_i=(f_1, f_2, ..., f_k)$, где $f_i \in F$. Согласно введенному определению пути, на графе этот путь представляет собой последовательность ребер и вершин $s_i=(...,v_0,E_0,v_1,E_1,...)$. Также имеет смысл ввести обозначение множества всех вершин, принадлежащих пути s_i, как V_{s_i}, и множества всех ребер, принадлежащих пути s_i, как E_{s_i}.

Рассмотренная модель киберфизической системы допускает моделирование сетей с учетом декомпозиции, модульности и возможных структурных изменений, позволяет проводить группировку функций по приведенным группам, а также отразить операционную модель атаки как воздействия на граф, описывающий КФС. При этом модель инвариантна к средствам им целям конкретной атаки или воздействия.

Компоненты обеспечения безопасности производственных систем.

Для определения места блока обеспечения безопасности в архитектуре цифрового производства определим его организацию в виде перечисленных ниже пунктов. В состав цифрового производства, с этой точки зрения, входят:

1. Архитектура цифровой инфраструктуры. Состав модулей и связей набора киберфизических объектов.

Архитектуру также можно разделить на набор составляющих. Например, современный интеллектуальный транспортный комплекс включает непосредственно систему управления беспилотным автомобилем, систему сбора и предобработки данных, контроля параметров, систему задания сценариев работы, систему управления сетью и управления конфигурацией, систему безопасности включая SIEM и блок принятия решений, и блок генерации сценариев ответного воздействия, связанный с системой конфигурации и генерирующий компенсирующие команды в случае фиксации воздействия.

2. Метод представления цифровой инфраструктуры или его модель. Для современных систем наиболее представительными с точки зрения обеспечения безопасности являются графовые модели. Пример такой модели приведен выше.

3. Общая модель киберфизической системы. Модель должна включать систематизацию компонентов системы, типы управления, особенности информационного управления и угрозы.

4. Умные средства автоматизации когнитивной обработки, самообучения и блоки самооценки прогноза состояния и принятия решений.

5. Магазин приложений. Набор интерфейсов для обмена с внешним миром в виде входящего и исходящего потока. Связь с другими системами для использования полученных результатов. Набор типовых приложений – сбыт, услуги, поставки, реклама.

6. Организация структур бизнес-модели.

7. Виртуальная общая шина системы передачи данных, включающая информационно – телекоммуникационную сеть, единую систему хранилищ данных.

8. Система обеспечения кибербезопасности. Общая структура контроля состояния киберфизической системы, обнаружения угроз, адаптивное управление устойчивостью универсальное понятие задач безопасности на уровне структуры блока порождающей модели и генератор моделей текущего состояния.

Для успешного функционирования необходимо достигнуть ряда факторов:

1. Безопасной среды функционирования системы защиты, включая компоненты мониторинга, оценки, принятия решения и генерации воздействия.

2. Выработка оценки безопасности состояния киберфизической системы, отвечающей требованиям современного цифрового производства и инвариантной к типу систем.

3. Определение методов прогнозирования и выработки решения.

Таким образом, система кибербезопасности должна включать компоненты сбора данных разного уровня с компонентов архитектуры, анализа информации, прогнозирования и выработки управляющих воздействий на основе механизма гомеостаза [6]. Для реализации описанного подхода необходимо иметь методы и средства прогноза изменения и состояния системы при влиянии внешней среды и изменении параметров.

Реализация системы прогнозирования ставит задачу создания цифрового двойника системы КФС и набора модулей и алгоритмов, позволяющих анализировать состояние системы, выбирать стратегию параметрических и структурных изменений, направленных на поддержание процессов функционирования КФС в соответствии с установленным критерием, и, если возможно, оптимизировать эти процессы хотя бы в схеме парето-оптимизации, т.е. режима не улучшаемых решений. Система обеспечения должна обладать значительной степенью интеллектуализации для того, чтобы решения принимались в режиме реального времени, без вмешательства оператора, роль которого сводится к контролю и выявлению аварийных ситуаций.

Обеспечение доверенной среды.

Для любых современных цифровых систем единственный способ обеспечить тотальность контроля – внедрение средств защиты на уровне операционной среды. Данный метод решения задачи воплощает системный подход к проблеме кибербезопасности и гарантирует достижение результатов, хотя и сопряжен с определенными затратами. Однако в этом случае затраты идут непосредственно на реализацию функций защиты, а не на переделку прикладных средств, неизбежно сокращающую их функциональные возможности, в процессе которой они к тому же успевают морально устареть. Напротив, доверенная среда будет актуальна до тех пор, пока существует проблема безопасности информационных технологий.

Создание доверенной среды подсистемы обеспечения информационной безопасности необходимо для ее успешного функционирования. В отношении киберсистем важным является обеспечение в этом вопросе технологической независимости. При этом широкое использование компонент различных производителей и международная интеграция производств, в том числе в области программного обеспечения, приводит к экономической неоправданности, а зачастую и к невозможности использования только отечественных программных средств.

В этой ситуации решением может стать предлагаемая авторами платформа на базе защищенной ОС «Фебос». Операционная система реализует гипервизор, изолирующий от непосредственного управления оборудованием пользовательские виртуальные машины, под управлением гостевых операционных систем. Гипервизор осуществляет мониторинг и реализацию функций безопасности операционной среды. Таким образом, на безе ОС «Фебос» формируется стек архитектурных и программных решений, контролирующих работу компонент различных производителей.

Возможными подходами к оценке безопасности киберфизических систем являются:

– нормативный подход, в соответствии с текущими стандартами и требованиями в области информационной безопасности. Однако на сегодняшний день отсутствует единый стандартизированный подход и методы оценки, в силу отставания нормативной базы от развития технологий;

– введение групп различных показателей для информационных и физических компонент системы;
– введение показателей, характеризующих состояние киберфизической системы в целом.

Индустриальные требования к кибербезопасности позволяют сформулировать общие требования к оценке безопасности киберфизических систем и производства в целом. Во-первых, оценка безопасности киберфизических систем должна быть инварианта к типу атаки. Во-вторых, она должна отражать операционный подход к модели атаки. Сложность киберфизических систем не позволяет, как было сказано выше, конкретизировать модель атаки полным перечислением, тогда как операционная модель позволяет, не идентифицируя тип атаки классифицировать воздействия по времени и степени влияния на систему.

Киберфизические системы имеют определенную скорость допустимой реакции на происходящие в них процессы. Следовательно, оценка безопасности должна вычисляться с достаточной скоростью, для того чтобы компенсирующее воздействие не запаздывало. Достижение этого требования зависит как от природы самой оценки, так и от построения системы анализа.

Разнообразие производственных систем, транспортных и экономических систем, сложность их организации в виде множества взаимодействующих компонент требуют дискретизации оценки: применимости ее как к системе в целом, так и к отдельным компонентам, для выявления слабых мест и проблем в больших промышленных комплексах.

В конечном итоге, оценка должна быть универсальна для всех типов систем и применима как для централизованных энергетических комплексов или SCADA, так и для распределенных систем VANET, FANET, MARINET, WSN, mesh, MANET, промышленного IoT. При этом она должна быть выражена в одном или нескольких количественных показателях, для адекватного сравнения безопасности систем и их компонент. Как следствие, оценка должна допускать применение прогнозирования, возможно в сочетании с другими параметрами КФС.

Прогнозирование и предотвращение деструктивных воздействий является одним из основных современных требований к системам управления безопасностью цифрового производства. В качестве подхода к оценке безопасности киберфизических систем, отвечающего заявленным требованиям, предлагается использовать показатель самоподобия системы. Таким образом, общая оценка устойчивости системы представляется оценкой ее текущего состояния безопасности, включая возможности прогнозирования безопасности будущих состояний, и характеристиками механизма выработки управляющего компенсирующего воздействия. Предлагается использование следующих показателей:

1. *Самоподобие* как степень сохранения работоспособности в условиях киберугроз в виде общей оценки безопасности;
2. *Устойчивость* системы как оценку зависимости работоспособности от интенсивности воздействий;
3. *Запас «живучести»* системы в условиях киберугроз как оценку возможности ее адаптации для сохранения самоподобия.

Под самоподобием системы понимается способность сохранять последовательность действий, необходимых для выполнения целевой функции, и наличие периодичности протекающих в ней процессов (выражающуюся в периодичности изменения параметров, характеризующих процессы), которые были бы инварианты к масштабу выполняемых действий.

Периодичность технологических процессов, реализуемых посредством передачи управляющего потока команд и сообщений между компонентами КФС, позволяет говорить о стационарности технологических процессов. Это означает, что свойства процесса, не меняются с течением времени, то есть, его характеристики инварианты относительно временных сдвигов, т.е. обладают свойством фрактальности или самоподобия.

Математически самоподобие технологического процесса КФС выражается через вычисление коэффициента Хёрста H над временными рядами $\frac{R}{S}=\left(\frac{N}{2}\right)^{H}$, где R – размах ряда, S -– стандартное отклонение, N – размер выборки.

При переходе от оценки состояния системы к комплексному пониманию ее безопасности необходимо определить запас «прочности» киберфизической системы к деструктивным внешним воздействиям. Свойство системы сохранять функционирование системы в заданном диапазоне входных и выходных характеристик в условиях целенаправленных внешних информационных воздействий называют киберустойчивостью, при чем в общем случае воздействия могут осуществляться как на информационном, так и на физическом уровне.

Подход на базе самоподобия предполагает оценку устойчивости за счет возможностей управления структурой и параметрами функционирования КФС. Основой подхода является оценка запасов избыточности киберфизической системы, за счет которых осуществляется компенсирующее воздействие, и возможности выработки такого воздействия. Согласно модели системы на базе функциональных графов и маршрутов можно выделить такие виды избыточности, как:

– параметрическая, выражающаяся в запасе диапазонов возможных значений параметров функционирования системы;
– функциональная, выраженная в функциональной избыточности узлов системы и возможности пере построения полезных маршрутов;
– структурная, выраженная в избыточности фактических узлов и связей системы.

Киберустойчивость системы связана с влиянием внешних факторов. Киберустойчивость является производной от самоподобия и может быть определена как способность сохранять самоподобие системы в условиях внешних воздействий. В этом контексте устойчивость соотносима с таким свойством системы, как управляемость.

Сохранение устойчивости системы может быть оценено на основе времени поиска альтернативного маршрута, реализующего данный киберфизический процесс, а также мощности множества релевантных маршрутов (избыточности системы). Определим два критерия способности системы к гомеостазу (способности сохранять устойчивое состояние):

1 $t_{search}(s_i) = \min(Search(s_i^{'}))$, где $Search(s_i^{'})$ - функция поиска маршрута, альтернативного маршруту si в системе и отвечающего набору правил R, где R - требования к маршруту. Требования к маршруту могут касаться использования (или неиспользования) отдельных вершин и связей, его временных характеристик и т.д.

2 $S_{sus}(s_i) = |S_{rel}|$, где $|S_{rel}| = \bigcup s_i^{'}$, то есть - мощность множества всех возможных альтернативных маршрутов в системе с учетом требований к маршруту R.

Указанные критерии применимы к каждому физическому процессу, происходящему в системе. Итоговая оценка системы может быть получена как $t_{search}^{\Sigma} = \max(t_{search}(s_i)), \forall s_i \in S$ и $S_{sus}^{\Sigma} = \min(|S_{rel}(s_i)|), \forall s_i \in S$.

Перспективы предлагаемого подхода:

1. Универсальность предлагаемой оценки самоподобия базируется на фундаментальных принципах методологии фрактального анализа и спектральных периодичностей, описывающих скрытые закономерности различных явлений безотносительно их природы.

2. Выявление нарушений на ранних стадиях попыток дестабилизации по изменению состояния системных связей, а не выявление отдельных типов атак.

3. Возможности создания систем с интеллектуальными методами автоматического поддержания самоподобия и оптимизации цифровых технологий на основе модели цифрового двойника.

4. Предлагаемые показатели самоподобия, устойчивости способности к гомеостазу составляют полную группу показателей, т.к. его защищенность по отношению к неизвестным типам воздействия.

5. Предлагаемый подход исходит из оценок состояния КФС, не требует настройки или адаптации к обнаружению конкретных видов атак, в том числе, к ранее неизвестным.

6. Предложенная система оценок самоподобия может быть использована для расширения возможностей различных SIEM и IDS, IPS систем в качестве критериев обнаружения аномалий.

Синтез компенсирующего воздействия.

Механизм выработки компенсирующего воздействия, определяющий наравне с избыточностью степень сопротивления и управляемости системы в условиях внешних деструктивных воздействий, может быть построен на базе гомеостатического подхода к управлению. Киберфизические системы полностью соответствуют гомеостатической концепции [7] иерархических систем с возможностью динамического изменения состава и архитектуры системы защиты, параметрической и структурной оптимизации и применения парето-оптимальных критериев для оценки текущего состояния.

Гомеостатическое управление представляет собой биоинспирированную концепцию управления интеллектуальными техническими системами и состоит в обеспечении относительного равновесия системы, поддерживаемого за счет механизмов саморегуляции. Гомеостаз подразумевает совокупность механизмов, обеспечивающих постоянство внутренней среды системы и структурно-функциональную устойчивость системы к внешним деструктивным воздействиям.

Реализация гомеостатической технологии управления осуществляется на основе специализированной подсистемы, называемой гомеостатом. Гомеостат- самоорганизующаяся система, направленная на поддержание значений ключевых параметров системы в границах множества допустимых значений. Предлагаемая структура гомеостата КФС состоит из трёх контуров управления: самоподобия временных рядов, характеризующих управляющий поток данных при реализации технологического процесса на параметрическом, структурном и функциональном уровнях.

В общем виде гомеостатическое управление устойчивостью и безопасностью всей КФС включает следующие этапы:

1. Мониторинг состояния системы и окружающей среды с целью обнаружения внешних воздействий, определением их направленности и специфики воздействия или фиксация фактов воздействия по изменению параметров системы в случае невозможности идентификации воздействия.

2. Анализ рисков воздействия, их последствий, подготовка данных для блока оценки состояния (идентификация воздействия, типизация сценария воздействия, механизмов, локализация механизмов).

3. Оценка изменения состояния системы, близости к критической области, локализация подсистем, потерявших работоспособность, оценка допустимой степени возможной потери функционала.

4. Генерация сценария гомеостатики для осуществления параметрических и структурных изменений, направленных на возвращение системы в область устойчивых состояний. Оценка рисков от частичной потери функционала и резервов для отражения следующих атак.

При выборе механизма гомеостаза можно исходить из принципов информационной безопасности – проводить оценку гомеостаза для заданного класса атак (модель угроз), механизмы атак (модель нарушителя), что требует экспериментов по моделированию типов и механизмов атак на базе принятой модели КФС.

В целом, исходя из механизмов гомеостаза, можно представить общий алгоритм гомеостатического управления, включающего оценку состояния и выработку, при необходимости, реакции.

Реализация гомеостатического управления на основе технологии ПКС

Технология ПКС изначально предложена в 2011 г. исследователями Стэнфордского университета и университета Беркли [8]. Основные концептуальные идеи технологии ПКС:

– отделение уровня управления от уровня передачи данных. Система управления является программной и реализуется на выделенном защищенном компьютере (контроллере ПКС);

– переход от управления отдельными единицами инфраструктуры к конфигурированию всей сети как единым целым, что призвано обеспечить комплексность и полноту применяемых правил над потоками данных и управления.

Основные функции контроллера ПКС:

– динамический анализ и фиксация состояния всех узлов киберсреды в данный момент времени.

– программное принятие решения об управлении узлами и потоками между ними в зависимости от состояния киберсреды, сетевых потоков, нагрузки, требований по безопасности, оказываемых воздействий и прочих управляющих факторов;

– задание конфигурации элементов киберсреды.

Поскольку функции управления становятся независимыми от различных производителей оборудования, доступными централизованно на прикладном (программном) уровне, подконтрольными разработчику программного обеспечения управления и реализуются с помощью технологии виртуализации сервисов безопасности (позволяет в виртуальной среде реализовывать функции принятия решений в зависимости от требований безопасности, предъявляемых к информационным потокам и потокам управления, от воздействий и принципов реагирования на инциденты), то можно утверждать о повышении безопасности, эффективности и гибкости управления киберсреды при использовании технологии адаптивных сетей и программного конфигурирования безопасности киберсреды.

Функционирование ПКС обеспечивает открытый протокол OpenFlow, через который осуществляется конфигурирование узлов киберсреды. Преимущество протокола OpenFlow – он не принадлежит конкретному производителю сетевого оборудования и является открытым стандартом.

Плоскость данных в любом узле управляемой киберсреды определяется таблицей сетевых потоков и действием, сопоставленным каждому правилу в данной таблице. Узлы, совместимые с протоколом OpenFlow, лишены функций управления. Без проприетарных протоколов управления, кроме открытого протокола OpenFlow, они становятся узлом, основная задача которого – пересылка пакетов между портами в зависимости от заданной контроллером ПКС таблицы сетевых потоков.

Каждая запись в таблице потоков имеет следующую структуру:

– правило выделения пакетов, принадлежащих данному потоку;

– действие, определяющие как должны быть обработаны элементы данного потока;

– статистика, которая отслеживает количество пакетов байтов данного потока, а также время, прошедшее с момента появления последнего пакета из данного потока, для удаления неактивных потоков.

Каждой записи в таблице сетевых потоков сопоставляется действие, которое должно быть применено к пакетам, принадлежащим данному потоку, в том числе:

– пересылка пакетов, принадлежащих данному потоку, далее на определенный порт или несколько портов (динамическая коммутация трафика);

– инкапсуляция и передача пакетов, принадлежащих данному потоку, на контроллер ПКС по безопасному каналу. Данное правило всегда применяется для первого пакета из нового потока, для того, чтобы контроллер ПКС принял решение о добавлении и направлении нового сетевого потока;

– отбрасывание пакетов, принадлежащих данному потоку. Данное правило может быть использовано для сдерживания кибератак типа «отказ в обслуживании» или фильтрации сетевого трафика в зависимости от изменяющихся условий и политик.

Для повышения сетевой безопасности масштабных систем и инфраструктур с изменяемой топологией разработана отечественная технология управления сетевыми инфраструктурами, которая позволяет объединить технологии гибридизации систем и технологии программно-конфигурируемых сетей (ПКС, Software Defined Networks, SDN) [9, 10].

Использование технологии гибридизации систем совместно с применением технологии управляемой (программно-конфигурируемой) безопасности позволяет реализовать множество сервисов управления (собственно управление, мониторинг, контроль) на одном контроллере ПКС, подключенном по протоколу OpenFlow к узлам киберсреды (рис. 2).

Архитектура виртуализированного контроллера ПКС, управляющего узлами киберсистемы, включает:

– настраиваемый виртуальный коммутатор на базе высокопроизводительного сервера;

– легковесное виртуальное окружение на базе гибридной системы;

– управляющие сервисы.

Достоинства такого решения:

– открытость платформы;

– унификация интерфейса управления;

– независимость от производителей ПО, оборудования, платформ и протоколов;

– повышение безопасности, улучшение контроля и мониторинга событий безопасности и состояний узлов всей системы;

– облегчение сертификационных исследований.

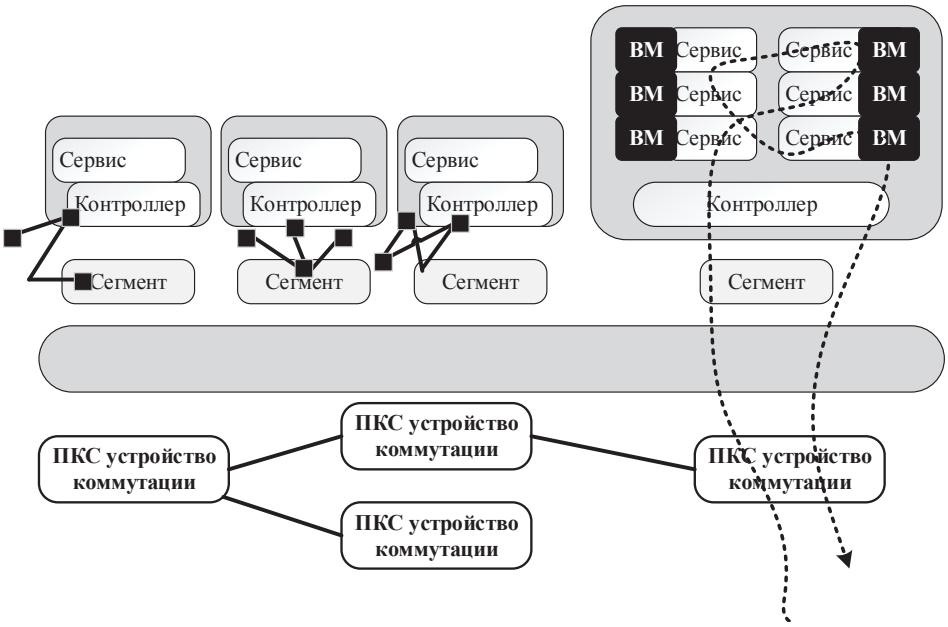


Рис. 2. Схема управления на базе технологии ПКС в гибридной виртуализированной системе контроллера ПКС (ВМ – виртуальная машина; базовая ОС – гипервизор)

Выводы.

1. Специфика защиты цифровых инфраструктур киберфизических систем от киберугроз состоит в том, что основной целью злоумышленников является вмешательство в физические процессы и управление цифровыми системами путем воздействия на информационные компоненты.

2. Для защиты киберфизических систем необходимы новые решения, основанные на конгломерате технологий блокчейн, больших данных, искусственного интеллекта, гомеостаза, ПКС, кибербезопасности направленных, в первую очередь, на обеспечение устойчивости функционирования и управления критическими системами в условиях постоянного воздействия целенаправленных киберугроз.

3. Возрастающая степень интеллектуализации киберсистем создает перспективы обеспечения устойчивости путем автоматизированного ситуационного управления с использованием цифрового двойника.

4. Предлагаемая система оценок устойчивости на основе самоподобия в совокупности с технологией гомеостатического управления дает возможность решать задачу противодействия киберугрозам.

При финансовой поддержке Министерства науки и высшего образования РФ в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014–2020 годы» (Соглашение от 03.10.2016 № 14.578.21.0224, уникальный идентификатор соглашения RFMEFI57816X0224).

СПИСОК ЛИТЕРАТУРЫ

1. Шваб К. Четвертая промышленная революция / К. Шваб — «Эксмо», 2016 — (Top Business Awards)
2. Industry 4.0 How to navigate digitization of the manufacturing sector // McKinsey Digital 2015 http://www.cloud-finder.ch/fileadmin/Dateien/PDF/Themenkategorien/industrie40/McKinsey_Report_Industry_4.0_s.pdf
3. Васильев Ю.С. Проблемы безопасности цифрового производства и его устойчивость к киберугрозам // Ю.С. Васильев, Д.П. Зегжда, М.А. Полтавцева. Проблемы информационной безопасности. Компьютерные системы. 2017. № 4. С. 47-63.
4. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf
5. Зегжда Д.П. Подходы к моделированию безопасности киберфизических систем Зегжда Д.П., Васильев Ю.С., Полтавцева М.А. Проблемы информационной безопасности. Компьютерные системы. 2017. № 3. С. 30-43.
6. Зегжда Д.П. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Вопросы кибербезопасности. 2018. № 2 (26). С. 2-15.
7. Зегжда Д. П., Павленко Е. Ю. Гомеостатическая стратегия безопасности киберфизических систем // Проблемы информационной безопасности. Компьютерные системы. 2017. № 3. С. 9-22.
8. M.O. Kalinin, E.Yu. Pavlenko. Increasing the Fault Tolerance and Availability of Software Defined Networks Using Network Equipment Control Based on Multiobjective Optimization by Service Quality Parameters / Automatic Control and Computer Sciences. – 2015. – Vol. 49, issue 8. – pp. 673-678.
9. M.O. Kalinin, V.M. Krundyshev, E.Yu. Rezedinova, D.V. Reshetov Hierarchical Software-Defined Security Management for Large-Scale Dynamic Networks / Automatic Control and Computer Sciences. – 2018. – Vol. 52, No. 8. – pp. 906-911.
10. P.D. Zegzhda, M.O. Kalinin Technology of Security Services Virtualization for High-Speed Computer Networks / Automatic Control and Computer Sciences. – 2016. – Vol. 50, No. 8. – pp. 734-738.

УДК 004.056.53

ЗАЩИТА ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ ОТ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Андреев Владислав Павлович, Черных Андрей Климентьевич
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: vl_pavl@mail.ru

Аннотация. В статье рассматриваются информационные угрозы для пользователей персональных компьютеров со стороны программ-вымогателей, профилактические меры и пути восстановления зашифрованных или заблокированных данных в случае заражения.

Ключевые слова: информационные угрозы; несанкционированный доступ; защита конфиденциальной информации; вредоносные программы; программы-вымогатели.

PROTECTING PERSONAL COMPUTERS FROM EXTORTION PROGRAMS

Andreev Vladislav, Chernykh Andrei
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mail: vl_pavl@mail.ru

Abstract. The article deals with information threats for users of personal computers from extortion programs, preventive measures and ways to restore encrypted or blocked data in case of infection.

Keywords: information threats; unauthorized access; protection of confidential information; malicious programs; extortion programs.

Введение.

В Доктрине информационной безопасности Российской Федерации указывается, что «одним из важных направлений обеспечения информационной безопасности в области науки, технологий и образования является обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности» [1].

В последние годы проблема защиты конфиденциальной информации от несанкционированного доступа стоит очень остро. Рассмотрим основные информационные угрозы для пользователей персональных компьютеров и меры по устранения этих угроз.

В основе атак на этих пользователей со стороны киберпреступников, чаще всего лежат финансовые соображения. Широкое распространение получили вредоносные программы, блокирующие работу компьютера или шифрующие на нем данные и требующие платы за коды для разблокировки.

Наиболее характерным примером подобных программ может служить троянская программа GPCode. Эта программа при заражении очередного компьютера устанавливала соединение с сервером и загружала на компьютер жертвы открытый ключ RCA, с помощью которого шифровала на нем данные. Для последующего зараженного компьютера создавался новый уникальный ключ. Соответственно закрытые ключи для расшифровки файлов были только у вымогателей. По оценке «Лаборатории Касперского» число уникальных IP-адресов компьютеров жертв, с которых были получены запросы на домены с sinkhole-серверами, составило 2764 в более чем 30 странах [2]. В последнее время подобные программы-вымогатели стали встречаться реже, поскольку перестали быть неожиданным «сюрпризом» для пользователей, которым уже известны соответствующие меры, которые необходимо предпринять для решения возникших проблем, поэтому появляются новые программы-вымогатели и их модификации - только за 2016 г. появилось 62 новых семейства этих программ и около 40 тысяч их модификаций [2].

Следует отметить, что злоумышленники стали использовать все более и более изощренные методы заражения, например, вредоносный код в виде аналитических скриптов на сайтах научных организаций для заражения устройств посетителей сайтов или вполне легальное программное обеспечение – средства администрирования, различные утилиты для оптимизации или автоматизации задач.

Так в 2016 г. было обнаружено целое семейство новых вымогателей PowerWare [3], использующих приложение Microsoft Office и утилиту PowerShell, входящую в состав операционной системы Windows. PowerWare загружается документом Word с макросами. Макросы используются для создания и запуска файла cmd.exe, который вызывает утилиту PowerShell с опциями, загружающими вредоносный код PowerWare.

Особую опасность представляют появившиеся в 2015 г. сервисы, работающие по модели Raas – «вымогательство как услуга», позволяющие любому пользователю, даже не имеющему соответствующего образования, зарегистрироваться на таких сервисах и приступить распространению троянских программ-вымогателей. Сервисы берут комиссию порядка 30% с каждой выплаты выкупа.

Опасность заключается в том, что «услугами» могут воспользоваться подростки или технически неподготовленные злоумышленники, действия которых могут привести к невозможности восстановления

информации в случае заражения. В качестве примера такого сервиса может служить сервис Satan, размещенный в анонимной сети The Onion Router, известной по аббревиатуре Tor.

Для предотвращения несанкционированного доступа к персональному компьютеру и риска утратить конфиденциальную информацию или заражения компьютеров программами-вымогателями в первую очередь надо соблюдать профилактические меры:

1. Выбор надежного интернет-сервиса. Защита данных пользователей без принятия соответствующих мер со стороны интернет-сервисов, используемых пользователями, – социальных сетей, электронной почты, облачных хранилищ и т.д., невозможна. Существующих в настоящее время способов защиты не всегда достаточно, хотя отдельные сервисы начали принимать дополнительные меры по защите своих клиентов, например, шифрование данных, передаваемых между собственными серверами.

2. Не использовать облачные хранилища в качестве резервных хранилищ конфиденциальных данных. Во-первых, информация, размещенная в «облаке», находятся в практически свободном доступе для разработчиков сервиса. Во-вторых, после совершения хакерской атаки на "облачный" сервис, не имеющий достаточно надёжной защиты от взлома, ваши данные могут быть похищены или уничтожены.

3. Основной способ защиты персонального компьютера или мобильного устройства – установка надежной антивирусной программы, способной предотвратить заражение. Современные, антивирусные продукты имеют систему предотвращения вторжений, блокирующую даже неизвестные версии троянцев, не позволяя им проникнуть в систему. Например, при атаке Gpcode при получении спамового письма с вложенным вредоносным DOC-файлом детектируется Trojan-Dropper.MSWord.Tored.a; компонент, загружающий Gpcode на компьютер, определяется как Trojan-Downloader.Win32.Small.crb. Сам Gpcode выявляется антивирусом. Работа без включенной антивирусной защиты, особенно с файлами из сомнительных источников, может закончиться безвозвратной утерей информации. Следите за тем, чтобы основные функции антивирусной программы, такие как Мониторинг активности, были всегда включены.

4. Регулярно создавать резервные копии данных, желательно на других устройствах.

5. Своевременно обновлять программное обеспечение на своем компьютере. В первую очередь это касается обновлений для установленной операционной системы, для систем безопасности приложений в составе операционной системы и средств удаления вредоносных программ. Обновления повышают совместимость программного обеспечения, установленного на компьютере, исправляют ошибки и уязвимости операционной системы.

6. Не открывать почтовые вложения и письма от незнакомых людей.

7. Хранить конфиденциальную информацию отдельно от остальных данных.

8. Не использовать открытые Wi-Fi-сети в общественных местах. При необходимости можно использовать только те названия сетей и пароли, которые вам предоставляют администраторы этих мест. При посещении сайтов, где вы не уверены в должной защите, в настройках включайте пункт «Всегда использовать безопасное соединение» (HTTPS).

Если вы все-таки стали жертвой программы-вымогателя и данные на вашем компьютере оказались зашифрованными, зайдите на сайт No More Ransom с незараженного компьютера.

В июле 2016 года Национальная полиция Нидерландов, Европол и компании Intel Security и «Лаборатория Касперского» создали некоммерческий проект «No More Ransom», с целью оказания помощи для восстановления заблокированных данных программами-вымогателями.

Кроме того, специалисты Лаборатории Касперского создали свои утилиты XoristDecryptor и RectorDecryptor для борьбы с этими программами. На рис. представлено окно утилиты XoristDecryptor.

Если запуск утилит не принесет результата, вредоносный файл будет отправлен на почту Лаборатории Касперского, где будет изучен специалистами и после найденного решения для его нейтрализации внесен в базу данных. Повторный запуск утилит должен устранить заражение.

Случаи блокировки компьютера баннерами с требованием отправить СМС для получения кода разблокировки менее опасны и, как правило, опытные пользователи могут самостоятельно разблокировать свой компьютер. Следует отметить, что в подобных случаях нет универсального способа решения. Поскольку злоумышленники постоянно модифицируют вредоносный код, то решения его нейтрализации зависят от каждого конкретного случая заражения.

Во всех случаях заражения блокируется практически весь компьютер, включая кнопку *Пуск* и *Диспетчер задач*.

Примерный алгоритм действий может быть следующим:

Перезагружаем компьютер в безопасном режиме и пробуем сделать откат системы. Помогает редко. Пробуем вызвать Диспетчер задач (при загрузке быстро нажимаем Ctrl+Alt+Delete) раньше, чем запуститься баннер. Если получиться, заходим в Процессы и завершаем новые незнакомые процессы. Пробуем определить имя процесса баннера (пропускаем некоторые процессы и смотрим, к чему это приведет, если баннера нет – перезагружаемся и т.д.).

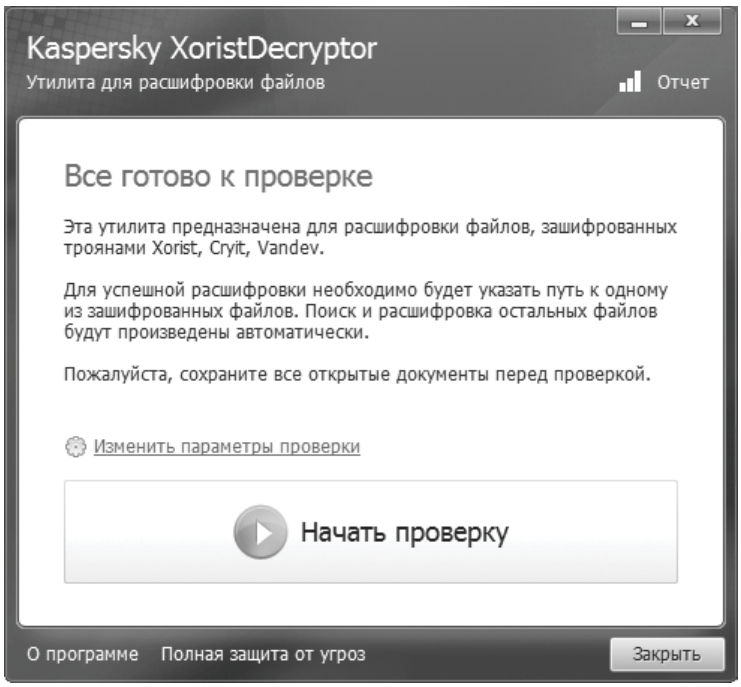


Рис.1. Окно утилиты XoristDecryptor

После определения имени процесса, осуществляем по нему поиск по всему компьютеру. При этом нужно обязательно включить показ скрытых файлов. Удаляем найденные файлы баннера. Если теперь заработает кнопка Пуск, выбираем в Пуске пункт Выполнить (Windows + R для Windows 10). В появившемся окне вводим команду msconfig. На рис. 2 представлено окно «Конфигурация системы», вызываемое командой msconfig. Выбираем закладку Автозагрузка. Проверяем свойства запущенных программ: имя, издателя и степень влияния активности. Отключаем подозрительные незнакомые программы. Запоминаем название и местоположения их файлов. После их удаления перезагружаем компьютер.

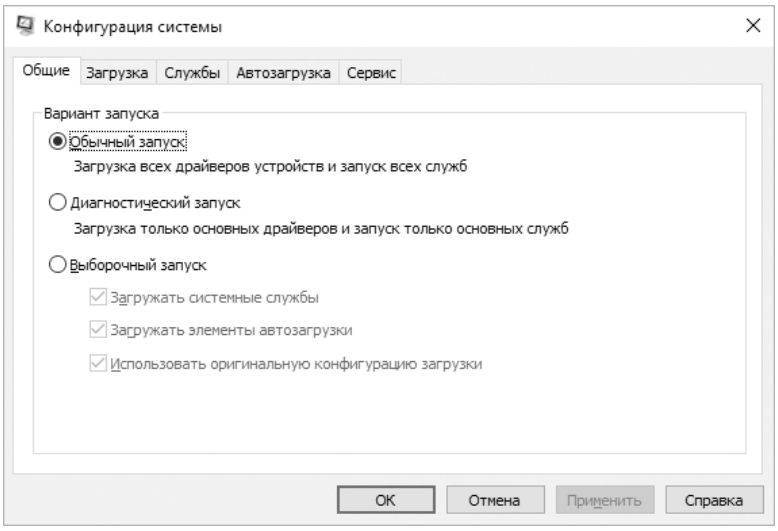


Рис. 2. Окно «Конфигурация системы», вызываемое командой *msconfig*

Для разблокировки диспетчера задач и редактора реестра можно воспользоваться специальными программами-разблокираторами, например, портативной версией Winhelper. Программа запускается поверх различных баннеров (режим "Поверх всех окон"). Вкладка Восстановление поможет восстановить редактор реестра, оболочку explorer.exe. Кроме того, во вкладке Автозагрузка можно просмотреть все запущенные программы.

Достаточно эффективным способом является использование загрузочных программ, например, WinDoza Live CD & USB, содержащих инструменты для восстановления операционной системы после блокировки баннером.

Пожалуй, самым простым способом избавиться от троянца-блокиратора, зайти с незараженного компьютера в базу кодов разблокировки «Доктор Web» по адресу https://www.drweb.com/xperf/unlocker/?lng=ru, на рис. 3 представлено окно сервиса разблокировки «Доктор Web», и, используя специальную форму, найти код разблокировки по номеру кошелька, телефону или изображению баннера.

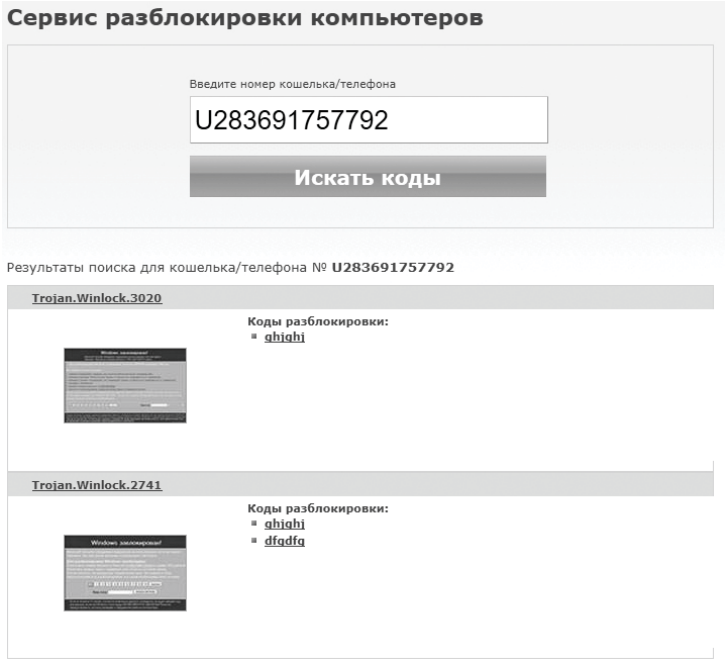


Рис. 3. Окно сервиса разблокировки «Доктор Web»

Важно отметить, что одной разблокировкой компьютера ограничиваться нельзя, необходимо удалить следы найденного троянца. Для этого можно воспользоваться бесплатной утилитой Dr.Web CureIt!, после чего зайти в реестр, вручную его проверить и остатки вируса удалить.

Заключение.

Таким образом, рассмотрены информационные угрозы для пользователей персональных компьютеров со стороны программ-вымогателей. Указаны профилактические меры необходимые для предотвращения несанкционированного доступа к персональному компьютеру, позволяющие снизить риск утраты конфиденциальной информации или заражения компьютеров программами-вымогателями. Представлены меры и пути восстановления зашифрованных или заблокированных данных в случае заражения компьютера.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации. Утверждена Указом президента Российской Федерации от 5 декабря 2016 г. №646.
2. Антон Иванов, Дэвид Эмм, Федор Синицын, Сантьяго Понтироли. Kaspersky Security Bulletin 2016. Сюжет года. Программы-вымогатели: революция. // [Электронный ресурс] – Режим доступа: https://securelist.ru/analysis/ksb/29788/kaspersky-security-bulletin-2016-story-of-the-year/
3. Mike Sconzo and Rico Valdez. Advanced Threat Protection, Detection and Response, Endpoint and Server Security, Mike Prevention, Ransomware, Response, Tech Toolbox. // [Электронный ресурс] – Режим доступа: https://www.carbonblack.com/2016/03/25/threat-alert-powerware-new-ransomware-written-in-powershell-targets-organizations-via-microsoft-word/

УДК 004.056.53

УГРОЗЫ ВЗЛОМА БЕСПРОВОДНЫХ СЕТЕЙ И МЕРЫ ПО ИХ ПРЕДОТВРАЩЕНИЮ

Андреев Владислав Павлович, Черных Андрей Климентьевич
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: vl_pavl@mail.ru

Аннотация. В данной статье рассматриваются информационные угрозы для пользователей персональных компьютеров использующих беспроводные сети и способы защиты этих сетей от несанкционированного подключения.

Ключевые слова: беспроводные сети; Wi-Fi; WEP; WPA; информационные угрозы; несанкционированный доступ; защита конфиденциальной информации; программы взлома.

THREATS OF WRAPPING OF WIRELESS NETWORKS AND MEASURES ON THEIR PREVENTION

Andreev Vladislav, Chernykh **Andrei**
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mail: vl_pavl@mail.ru

Abstract. The article considers information threats for users of personal computers using wireless networks and ways to protect these networks from unauthorized connection.

Keywords: wireless networks; Wi-Fi; WEP; WPA; information threats; unauthorized access; protection of confidential information; hacking programs.

Беспроводные сети, называемые также Wi-Fi (Wireless Fidelity) или WLAN (Wireless LAN) прочно вошли в нашу жизнь и получили широкое распространение во всем мире.

В настоящее время для защиты беспроводных сетей применяются сложные алгоритмические и математические методы аутентификации, шифрования и контроля целостности передачи данных. Тем не менее, для перехвата сетевого трафика беспроводных сетей этих методов оказывается часто недостаточно. Неправильные настройки шифрования на точке доступа или передача информации в открытом виде приводит к тому, что для подключения к сети злоумышленнику достаточно иметь ноутбук с беспроводным адаптером и расположиться вблизи точки доступа.

Использование устаревшего протокола WEP (Wired Equivalent Privacy) для шифрования данных в беспроводных сетях сегодня встречается редко. В WEP используется симметричная схема шифрования, использующая алгоритм RC4. Защита беспроводной сети, построенная на использовании WEP с аутентификацией по MAC-адресу и статическими ключами неустойчива к существующим методам взлома и практически равноценна использованию открытых сетей [1].

Более поздний протокол Wi-Fi Protected Access (WPA), вытеснивший протокол WEP, использует технологию динамической генерации ключей шифрования данных на базе протокола TKIP (Temporal Key Integrity Protocol). Кроме того, этот протокол поддерживает шифрование по усовершенствованному стандарту AES (Advanced Encryption Standard) с более стойким криптоалгоритмом по сравнению с протоколами WEP и TKIP.

При использовании в стандарте WPA протокола аутентификации EAP пользователь обязан подтверждать свое право на доступ в сеть. В настоящее время семейство WPA считается наиболее защищенным от взлома и подавляющее число точек доступа использует основанное на нем шифрование. Самый высокий уровень защиты данных и доступа в беспроводную сеть имеет вторая версия этого протокола WPA2 [2].

Шифрование трафика на точках доступа сегодня считается необходимым условием для защиты конфиденциальных данных при использовании беспроводных сетей [3]. Но насколько оно эффективно? Приведем пример: по данным компании Group-IB в период с 2015 г. по начало 2016 г. у пользователей Wi-Fi , было похищено 348 млн. рублей, юридических лиц через мобильный банк 956 млн. рублей. Количество взломов беспроводных сетей ежегодно увеличивается, и большинство этих случаев остается вне статистики.

При попытках несанкционированного подключения к беспроводным сетям злоумышленники используют два основных метода взлома сетей. Наиболее простой и распространенный, Brute Force (метод «грубой силы») использует перебор паролей. При его использовании запускается специальная программа для взлома и вводится интересующая злоумышленника сеть. Время взлома в основном зависит от сложности и длины пароля.

Для сокращения времени перебора используются словари паролей. Поскольку большинство пользователей используют в составе готовые слова, то их перебор занимает намного меньше времени, чем перебор случайных символов.

В интернете можно найти и скачать «брутфорсы» любых типов: для серверов, почты, ICQ, сайтов и т.д. На рис. 1 представлены брутфорсы различных типов.

Рис.1. Брутфорсы различных типов

Если для взлома сложного пароля требуется значительное время, то используются специальные программы для перехвата пакетов между компьютером и роутером. После расшифровки данных пакетов, взломанный пароль злоумышленник может отправить либо себе на почту, либо на удаленный сервер. В качестве примера подобных программ может служить программа Wihack. На рис. 2 представлена программа Wihack для взлома Wi-Fi.

http://spoisu.ru

Рис.2. Программа Wihack для взлома Wi-Fi

При обнаружении беспроводных сетей программа анализирует их на наличие защищенности, позволяет получить список пользователей сети, подобрать пароль к Wi-Fi, осуществить перехват пакетов и выявить, чем занимается пользователь, при желании заблокировать работу этого пользователя. Подобными программами могут воспользоваться злоумышленники даже, не имеющие специального технического образования.

Более «продвинутые» злоумышленники используют пакеты различных программ, чаще всего CommView for Wi-Fi и Aircrack-ng (для операционной системы Windows последняя версия 0.9.3-win).

Программа CommView for WiFi может перехватывать сетевые пакеты и получать подробную информации о сети: список точек доступа и узлов, статистику по каждому узлу и каналу, уровень сигнала, список пакетов и сетевых соединений и т.д.

Программа Aircrack осуществляет перехват пакетов в защищенной WEP или WPA шифрованием беспроводной сети для последующего анализа и расшифровки. После замены штатных драйверов от производителя беспроводного сетевого адаптера на специальные драйверы, поддерживающие режим мониторинга и перехвата пакетов запускается файл Aircrack-ng GUI.exe, представляющий собой графическую оболочку для утилит, входящих в пакет Aircrack-ng. На рис.3 представлено окно программы Aircrack-ng.

Процедура взлома беспроводной сети выполняется в три этапа: сбор информации о сети, перехват пакетов и их анализ.

Использование программы Aircrack-ng показывает, что часто рекомендуемые способы защиты беспроводных соединений: использование режима с использованием режима скрытого идентификатора сети (Hide SSID) и фильтрация по MAC-адресам не эффективны. Утилита airodump-ng также, как и программа CommView for Wi-Fi показывают SSID сети, который можно будет использовать для дальнейшего подключения к сети. Что касается фильтрации по MAC-адресам, то подменить MAC-адрес сетевого интерфейса можно с помощью программ, которые можно найти в Интернете, например, MAC MakeUP, Ryll MAC Edito и т.д.

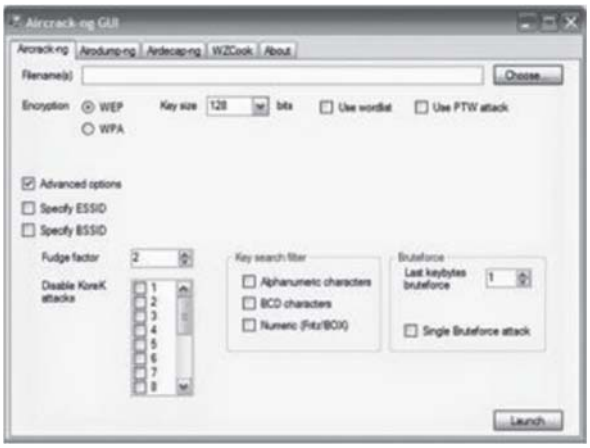


Рис.3. Программа Aircrack-ng

Для защиты беспроводных сетей от взлома и от утраты конфиденциальной информации можно рекомендовать следующие меры (следует иметь в виду, что гарантии 100% защиты от взлома нет):

– При выборе пароля сети не используйте короткие пароли и слова, имеющие смысл.

– Всегда выключайте соединение Wi-Fi, когда вы им не пользуетесь. Кроме того, отключите функцию автоматического подключения к имеющимся Wi-Fi соединениям.

– Если есть сомнения в безопасности используемой вами беспроводной сети, но есть необходимость выйти в интернет, используйте только простые действия, не вводите логины и пароли сервисов и не совершайте любые операции в онлайн-банке.

– Не пользуйтесь конфиденциальной информацией в общественных местах: кафе, вокзалах, автостоянках и т.д., даже если названия сетей и пароли вам предоставят работники данного заведения. Злоумышленники могут выяснить пароли этих сетей, а затем создать фальшивые соединения с такими же паролями.

– При посещении сайтов, где вы не уверены в должной защите, в настройках включите пункт «Всегда использовать безопасное соединение» (HTTPS).

– Если есть возможность, используйте подключение через виртуальную частную сеть (VPN), трафик в которой маршрутизируется по защищенному туннелю в зашифрованном виде.

– Используйте программные средства для обнаружения несанкционированного доступа к вашей беспроводной сети. Например, свободно распространяемая программа SoftPerfect WiFi Guard осуществляет сканирование вашей сети и дает информацию обо всех подключенных устройствах. На рис. 4 представлено окно программы SoftPerfect WiFi Guard.

– Фильтрация MAC-адресов не позволяет защитить сеть, но в какой-то мере может повысить уровень ее безопасности, например, оградит от соседей. Это касается и режима скрытого идентификатора, при котором сеть не отображается в списке доступных сетей.

– Используйте специализированные решения защиты беспроводных соединений, например, функцию «Безопасное соединение», реализованную в Kaspersky Internet Security и Kaspersky Total Security. Указанный модуль предоставляет пользователю безопасный зашифрованный канал связи при переходе на сайты онлайн-банкинга, платежных систем и т.д.

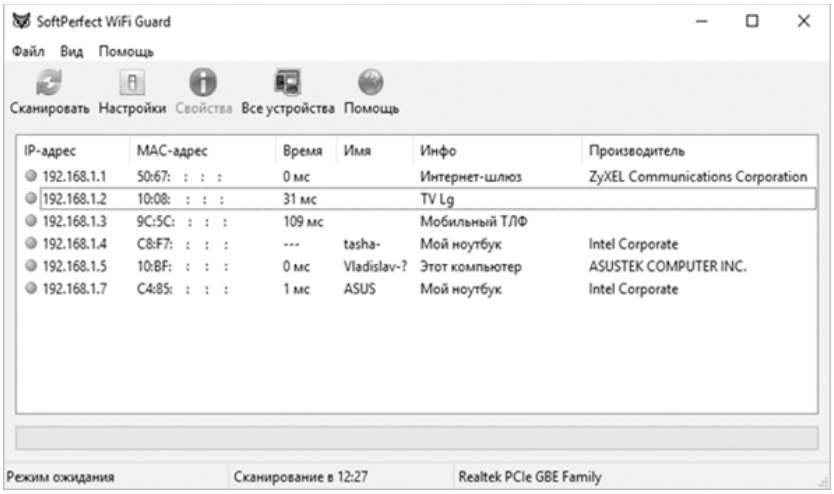


Рис.4. Окно программы SoftPerfect WiFi Guard

СПИСОК ЛИТЕРАТУРЫ

1. Маркелов К. С., Нейман А. Б. Безопасность беспроводных сетей // Молодой ученый. — 2012. — №4. — С. 63-66.
2. Патий Е. Проблемы безопасности в беспроводных сетях/ Е.Патий // Искусство управления информационной безопасностью [Электронный ресурс]. – Режим доступа: http://www.iso27000.ru/chitalnyi-zai/bezopasnost-besprovodnyh-setei/problemy-bezopasnosti-v-besprovodnyh-setyah/.
3. Андрушка Игорь // Лаборатория Информационной безопасности. [Электронный ресурс]. – Режим доступа: http://security.ase.md/publ/ru/pubru79/.

УДК 004.056.5

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ЯЗЫКА RUBY И ФРЕЙМВОРКА RAILS И МЕТОДЫ ИХ РЕШЕНИЯ

Жарков Арсений Дмитриевич, Савков Сергей Витальевич, Садикова Анастасия Александровна
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: arsenzhar@gmail.com, sergsavkov@gmail.com, anastasiiasad1004@gmail.com

Аннотация. В данной статье представлены проблемы безопасности, с которыми могут столкнуться разработчики и пользователи Ruby on Rails приложений, и методы их решения. Как и в большинстве языков программирования, в Ruby существуют библиотеки, которые написаны сообществом – gems. Использование сторонних библиотек является одной из проблем безопасности Ruby-приложений. В данной статье приведены методы защиты от возможных уязвимостей сторонних библиотек. Следующей является проблема безопасной реализации многопоточности (Thread Safe). При работе с переменными или данными из базы данных в потоках, возникает проблема изменения этих данных при параллельном выполнении. В данной статье приведены методы,

позволяющие избегать конфликтов в потоках. Также рассматривается проблема, связанная с состоянием гонки, которое возникает, когда на сервер поступает несколько запросов одновременно (Race Condition). При одновременной обработке двух запросов, которые работают с одними данными, результат последнего запроса зависит от результата первого. В статье рассказывается, как избежать Race Condition в Ruby.

Ключевые слова: Ruby on Rails; языки программирования; безопасность

RUBY LANGUAGE SECURITY PROBLEMS AND RAILS FRAMEWORK AND METHODS OF THEIR SOLUTION

Zharkov Arseny, Savkov Sergey, Sadikova Anastasia
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics
(University ITMO)
49 Kronverksky Av., St. Petersburg, 197101, Russia
e-mails: arsenzhar@gmail.com, sergsavkov@gmail.com, anastasiiasad1004@gmail.com

Abstract. This article presents security issues that developers and users of Ruby on Rails applications may encounter, and methods for solving them. As in most programming languages, there are libraries in Ruby that are written by the community - gems. Using third-party libraries is one of the security concerns of Ruby applications. This article provides methods for protecting against possible vulnerabilities in third-party libraries. The next is the problem of safe threading implementation. When working with variables or data from a database in streams, the problem arises of changing this data during parallel execution. This article provides methods for avoiding conflicts in threads. It also addresses the problem of the race condition, which occurs when several requests are sent to the server at the same time (Race Condition). When simultaneously processing two queries that work with the same data, the result of the last query depends on the result of the first. This article explains how to avoid Race Condition in Ruby.

Keywords: Ruby on Rails; programming languages; security

Введение.

В современном мире существует множество языков программирования и фреймворков, предназначенных для написания веб-приложений. Одним из таких языков является Ruby, который стал популярным благодаря веб-фреймворку Rails.

Ruby – интерпретируемый язык программирования высокого уровня. Он обладает простым синтаксисом и является полностью объектно-ориентированным языком программирования – Все данные в Ruby являются объектами. Для любой информации или кода могут быть определены свои свойства и методы. Ruby очень гибкий язык, он позволяет программисту легко переопределять методы.

Rails – фреймворк с открытым кодом, написанный на языке Ruby. Rails реализует архитектурный шаблон Model View Controller (MVC) для веб-приложений, легко интегрируется с веб-сервером и имеет собственную ORM – ActiveRecord.

Согласно данным аналитики, Ruby on Rails входит в 5 наиболее используемых фреймворков для веб-разработки и его популярность стремительно возрастает. Зачастую развитие языка Ruby опережает развитие основанных на нём технологий. Таким образом существует актуальная проблема обеспечения безопасности веб-приложений, использующих данный стек технологий. Данная статья посвящена проблемам безопасности языка Ruby и наиболее актуальным уязвимостям Ruby on Rails приложений.

Уязвимости сторонних библиотек

Специфичным для Ruby-приложений является модульная структура, то есть используется множество сторонних библиотек (gems). С одной стороны, это упрощает разработку, а с другой несёт в себе скрытые угрозы безопасности, которые по факту порождаются внутренними уязвимостями этих библиотек. Часто иерархия зависимостей является достаточно сложной для отслеживания уязвимостей сторонних модулей в ручном режиме. Например, для работы с внешним хранилищем файлов (AWS) популярным решением является использование библиотеки Paperclip. Для данной библиотеки возможна атака Server Side Request Forgery, позволяющая инициировать запросы с атакуемого хоста на другие компоненты системы. Дальнейшее исследование дерева зависимостей показывает, что Paperclip использует библиотеку libxml2, которая также содержит в себе ряд уязвимостей. Наиболее эффективным подходом к защите от подобных уязвимостей является постоянный мониторинг открытых репозиториев уязвимостей и актуализация версий библиотек. К сожалению, любое обновление сложной структуры зависимостей само по себе является угрозой выхода системы из строя. Поэтому задача актуализации библиотек, в зависимости от критичности выявленных уязвимостей и их устранения, решается сторонними инструментами на основе открытых баз данных уязвимостей (CVE). Одним из таких инструментов является Bundler-audit, который анализирует файл Gemfile.lock, содержащий список всех используемых библиотек с указанием версий, и сверяет с базой данных угроз. Если в проекте используются устаревшие версии gems, которые содержат в себе уязвимости, являющиеся критичными, Bundler-audit сообщит об этом и предложит использовать актуальную версию.

Использование сторонних библиотек также порождает проблему доверия к источникам (репозиториям), хранящим их исходные коды. В случае использования недоверенных источников, возникает вероятность подмены библиотек. На сегодняшний день большинство gems хранятся в репозиториях хостинга RubyGems.org. Данный сервис предоставляет механизм проверки подписи репозитория, а также возможность верификации изменений кода библиотек перед применением изменений в рамках основной ветки. К сожалению, данный подход предполагает

доверие к владельцу репозитория и не обеспечивает безопасность в случае необходимости использования библиотек, недостаточно апробированных Ruby-сообществом. Здесь единственной альтернативой для разработчика является отказ от готового решения и разработка данного функционала своими силами.

Безопасность многопоточных Ruby-приложений.

Достоинством Ruby-приложений является возможность реализации многопоточного режима. Это позволяет наиболее эффективно использовать системные ресурсы посредством распараллеливания вычислительных задач. Обратной стороной многопоточности являются риски, связанные с совместным использованием данных и синхронизацией потоков. Например, таким риском является непредсказуемость результата, связанная с отсутствием блокировок данных и одновременной записью в базу данных из нескольких потоков.

Минимизировать риски из данного класса возможно, применяя при разработке набор соглашений thread-safe, включающий следующие рекомендации:

1. Избегать использование общих переменных, с которыми могут работать несколько потоков.
2. Использовать локальные переменные потока, вместо работы через указатели.
3. Избегать сдвоенных операций, например, ||=.
4. Тщательно проверять код библиотек.

Подход thread-safe должен применяться на всех уровнях приложения ко всем его компонентам:

- Фреймворк Rails должен быть thread-safe.
- Написанный разработчиком код должен быть thread-safe.
- Все сторонние библиотеки должны быть thread-safe.

На сегодняшний день Rails и все библиотеки, включённые в фреймворк по умолчанию, являются потокобезопасными. Также начиная с Rails 4.0 (сейчас актуальной версией является Rails 5.2), функция thread-safe включена по умолчанию, что позволяет приложению использовать возможности веб-сервера Puma, который поддерживает многопоточность и поставляется с Rails. Rails создаёт новый объект контроллера для каждого HTTP-запроса, это изолирует большинство объектов в приложении от других запросов. Поэтому потокобезопасность приложения определяется преимущественно кодом контроллера.

В Ruby все структуры данных, кроме очередей, не являются потокобезопасными, поэтому чтобы написать thread-safe приложение, необходимо избегать использование переменных в потоках. Существует три типа переменных:

- глобальные переменные;
- переменные класса;
- переменные экземпляра класса.

Глобальные переменные доступны из любого места программы, поэтому их изменение в потоке делает приложение не thread-safe, соответственно их использование является крайне нежелательным.

Переменные класса и переменные экземпляра класса во многом сходны с глобальными переменными (если речь идёт об использовании их в потоках), поэтому если переменная не изменяется, лучше использовать константы. Также переменные могут определяться с помощью методов класса.

Для присвоения значения переменным часто используется «ленивая инициализация», посредством конструкции вида ||=, которая объединяет две операции, что автоматически делает код не thread-safe.

Третим пунктом является потокобезопасность сторонних библиотек: чтобы приложение было полностью потокобезопасным, необходимо, чтобы каждый компонент был thread-safe. Поэтому код сторонних библиотек должен быть тщательно изучен перед использованием в многопоточном приложении.

Угрозы, связанные с проблемой Race Condition.

Race Condition или состояние гонки рассматривается с точки зрения совместных операций с базой данных и параллельной обработкой нескольких запросов, что может привести к непредсказуемости результата. Чтобы этого избежать, необходимо каждый запрос к базе данных оборачивать в отдельную транзакцию при параллельной работе нескольких потоков.

Заключение.

В данной статье была обозначена специфика безопасности Web-приложений, написанных на языке Ruby с использованием фреймворка Rails:

1. Модульная структура Ruby-приложений предполагает использование сторонних библиотек, которые могут содержать в себе скрытые уязвимости. Для снижения рисков необходимо верифицировать источники библиотек, а также проверять используемые библиотеки на наличие известных уязвимостей.

2. Ruby изначально не обеспечивает потокобезопасность, поэтому при написании многопоточных приложений важно следовать концепции thread-safety.

3. Для многопоточных приложений также актуальна проблема неопределенности параллелизма (Race Condition). Ее решение заключается в реализации транзакционности запросов приложения к БД.

СПИСОК ЛИТЕРАТУРЫ

1. Ruby gems are still not safe to use [Электронный ресурс] // Cristiano Betta, Developer Experience consultant. – Режим доступа: https://betta.io/blog/2013/02/02/ruby-gems-are-not- safe-to-use/, свободный (дата обращения: 10.05.2018).
2. How Do I Know Whether My Rails App Is Thread-safe or Not? [Электронный ресурс] // Bear Metal. – Режим доступа: https://bearmetal.eu/theden/how-do-i-know-whether-my-rails- app-is-thread-safe-or-not/, свободный (дата обращения: 15.05.2018).
3. Avoid race conditions in Rails with Postgres locks [Электронный ресурс] // Leigh Halliday. – Режим доступа: https://www.leighhalliday.com/avoid-race-conditions-with- postgres-locks, свободный (дата обращения: 23.05.2018).

УДК 681.3

ПОСТКВАНТОВЫЙ АЛГОРИТМ ЦИФРОВОЙ ПОДПИСИ, ОСНОВАННЫЙ НА СКРЫТОЙ ЗАДАЧЕ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ

Молдовян Николай Андреевич[1], Абросимов Иван Константинович[2]

[1] Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия В.О., 39, Санкт-Петербург, 199178, Россия
[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: nmold@mail.ru, ivnabr@yandex.ru

Аннотация. Предложено построение схем цифровой подписи на основе вычислительной трудности скрытой задачи дискретного логарифмирования, задаваемой над конечными ассоциативными алгебрами с некоммутативной операцией умножения. Рассмотрена 4-мерная алгебра указанного типа и описаны ее свойства, используемые при построении криптосхем.

Ключевые слова: постквантовая криптография; криптографические примитивы; схемы электронной цифровой подписи; конечные алгебраические структуры.

POST-QUANTUM DIGITAL SIGNATIRE PROTOCOL BASED ON THE HIDDEN DISCRETE LOGARITHM PROBLEM

Moldovyan Nikolay[1], Abrosimov Ivan[2]

[1] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th liniya, Vasilievsky Island, St. Petersburg, 199178, Russia
[2] Saint Petersburg Electrotechnical University «LETI»
5 Professor Popov Str., St. Petersburg, 197376, Russia
e-mails: nmold@mail.ru, ivnabr@yandex.ru

Abstract. The design of the digital signature schemes based on computational difficulty of the hidden discrete logarithm problem defined over the finite associative algebras with non-commutative multiplication operation is proposed. There is considered the 4-dimensional algebra of the indicated type. Properties of the last one, which are used at constructing the signature scheme are considered.

Keywords: post-quantum cryptography; cryptographic primitives; digital signature schemes; finite algebraic structures.

Введение.

В настоящее время наиболее широкое практическое применение для открытого распределения ключей, открытого шифрования и формирования электронных цифровых подписей (ЭЦП) в современных информационных системах получили протоколы криптографии с открытым ключом, основанные на вычислительно трудных задачах факторизации (ЗФ) и дискретного логарифмирования (ЗДЛ) [1]. Безопасность протоколов данного вида основана на том, что в настоящее время лучшие алгоритмы решения указанных задач имеют сверхполиномиальную вычислительную сложность при использовании лучших известных алгоритмов, разработанных для современных универсальных ЭВМ. В связи со становлением и прогрессом в развитии квантовых вычислителей, представляющих собой аналоговые ЭВМ, в которых вычислительный процесс задается свойствами квантовой системы, и позволяющих чрезвычайно эффективно решать частные задачи дискретной математики, возникла актуальная проблема оценки стойкости криптосхем, основанных на ЗДЛ и ЗФ, к атакам с применением гипотетического квантового компьютера.

В работах [2,3] показано, что каждая их упомянутых двух задач имеет полиномиальную сложность при ее решении на квантовом компьютере. Этот результат означает, что в случае появления практически значимых квантовых вычислителей действующие в настоящее время стандарты, регламентирующие использование двухключевых криптографических алгоритмов и протоколов, должны быть отменены как не обеспечивающие требуемый уровень стойкости. Последнее порождает проблему развития арсенала алгоритмов ЭЦП, протоколов открытого распределения ключей, открытого шифрования и ЭЦП, которые были бы безопасными в случае появления возможности практического использования квантовых вычислителей для выполнения атак на криптосхемы.

Для обеспечения достаточно высокого уровня стойкости алгоритмов и протоколов двухключевой криптографии требуется положить в их основу вычислительно трудные задачи, вычислительная сложность решения которых является сверхполиномиальной как при решении на компьютерах обычного типа, так и при их решении на квантовых компьютерах. Высокая степень актуальности разработки алгоритмов и протоколов постквантовой криптографии обусловила появление регулярно проводимых тематических конференций [4,5] и объявление Национальным институтом стандартов и технологий (НИСТ, National Institute of Standards and Technology, NIST) конкурса на разработку постквантовых криптосхем с открытым ключом [6,7].

Перспективное направление построения постквантовых двухключевых криптосхем связано с использованием вычислений в некоммутативных алгебраических структурах. В качестве базового

криптографического примитива в таких криптосхемах используется так называемая ЗДЛ в скрытой циклической группе (или просто скрытая ЗДЛ). Ранее были предложены протоколы открытого распределения ключей, открытого шифрования и алгоритм коммутативного шифрования, основанные на скрытой ЗДЛ [8]. Однако не были известны протоколы ЭЦП, основанные на этой задаче. При этом ранее было известно весьма ограниченной число конечных некоммутативных алгебр, которые могут служить в качестве носителя скрытой ЗДЛ.

В настоящей работе предлагается решение задачи построения схем ЭЦП на основе скрытой ЗДЛ, рассматривается вопрос построения новых конечных некоммутативных алгебр с ассоциативной операцией умножения и описываются их свойства, связанные с заданием скрытой ЗДЛ, причем для обеспечения возможности разработки схем ЭЦП предлагается новая форма скрытой ЗДЛ.

Криптосхемы на основе комбинирования операций возведения в степень и сопряжения. Известно, что в конечной некоммутативной группе Γ функция отображения группы на себя, задаваемая формулой $\varphi_X(\mathbf{G}) = \mathbf{X} \circ \mathbf{G} \circ \mathbf{X}^{-1}$, где $\mathbf{X}$ – фиксированный элемент группы Γ и $\mathbf{G}$ – элемент, пробегающий все значения в группе Γ, задает автоморфное отображение [9]. Преобразование, определяемое последней формулой, называется операцией сопряжения, а элементы $\mathbf{G}$ и $\mathbf{Y} = \mathbf{X} \circ \mathbf{G} \circ \mathbf{X}^{-1}$ – сопряженными через элемент $\mathbf{X}$. Для фиксированного значения $\mathbf{X}$ операция вычисления сопряженного элемента и операция возведения в степень являются перестановочными (взаимно коммутативными) [9], т. е. имеет место соотношение $\varphi_X(\mathbf{G}^x) = (\varphi_X(\mathbf{G}))^x$. Это свойство может быть использовано для формулирования следующей вычислительно трудной задачи, пригодной для использования в качестве примитива криптосистем с открытым ключом.

Пусть выбран элемент $\mathbf{G} \in \Gamma$, порядок которого равен достаточно большому простому числу. Пусть выбран элемент $\mathbf{X} \in \Gamma_{комм} \subset \Gamma$ такой, что $\mathbf{X} \circ \mathbf{G} \neq \mathbf{G} \circ \mathbf{X}$, где $\Gamma_{комм}$ – коммутативная группа большого порядка, задано некоторое целое число x и вычислен элемент $\mathbf{Y} = \mathbf{X} \circ \mathbf{G} \circ \mathbf{X}^{-1}$. Скрытая ЗДЛ в известной форме формулируется следующим образом: по заданным $\mathbf{Y}$ и $\mathbf{G}$ требуется вычислить $\mathbf{X}$ и x [10].

На основании скрытой ЗДЛ можно построить протоколы открытого распределения ключей и бесключевого шифрования. Для реализации данных криптосхем в работах [11,12] предложено использовать конечные группы матриц размерности 2×2 и конечные группы четырехмерных векторов, заданных над простым полем $GF(p)$. В работе [13] было показано, что для случаев использования некоммутативных групп двух последних видов задача дискретного логарифмирования в скрытой циклической подгруппе сводится к задаче дискретного логарифмирования в расширенном поле $GF(p^2)$. Такое сведение показывает, что для разработки постквантовых криптосхем на основе комбинирований операций автоморфного отображения и возведения в степень следует попытаться использовать некоммутативные конечные группы других типов и новые формы скрытой ЗДЛ.

Алгебраический носитель для новой формы, скрытой ЗДЛ. В качестве алгебраической структуры, на основе которой можно было бы сформировать скрытую ЗДЛ, предлагается конечная некоммутативная алгебра с ассоциативной операцией умножения векторов. Результат умножения векторов в этой алгебре определяется по правилу перемножения каждой компоненты первого вектора с каждой компонентой второго вектора. После раскрытия скобок выполняется замена в каждом слагаемом произведения пар базисных векторов на однокомпонентный вектор в соответствии с так называемой таблицей умножения базисных векторов [12]. Строкам и столбцам данных таблиц соответствуют базисные вектора, а ячейкам – результат их перемножения. Результатом перемножения является некоторый базисный вектор, умноженный на структурный коэффициент. Структурные коэффициенты принадлежат конечному полю, из которого берутся координаты векторов.

Примером описанной конечной некоммутативной алгебры с ассоциативной операцией умножения векторов может служить алгебраическая структура, ТУБВ которой представлена на рис. 1.

$\circ$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{e}$	$\mathbf{e}$	$\alpha\mathbf{k}$	$\alpha\mathbf{e}$	$\mathbf{k}$
$\mathbf{i}$	$\beta\mathbf{j}$	$\mathbf{i}$	$\mathbf{j}$	$\beta\mathbf{i}$
$\mathbf{j}$	$\mathbf{j}$	$\alpha\mathbf{i}$	$\alpha\mathbf{j}$	$\mathbf{i}$
$\mathbf{k}$	$\beta\mathbf{e}$	$\mathbf{k}$	$\mathbf{e}$	$\beta\mathbf{k}$

Рис.1. Строение ТУБВ для задания ассоциативной операции умножения четырехмерных векторов

Для построения криптографических схем необходимо определить критерий необратимости векторов по операции умножения, заданной ТУБВ. Данный критерий для рассматриваемой алгебраической структуры получается путем решения систем линейных уравнений (1) и (2) относительно x, y, z, w.

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}) = (a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}), \quad (1)$$

$$(x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}) \circ (a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = (a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}), \quad (2)$$

Главные определители системы (1) и (2) позволяют сформулировать критерий (3) обратимости произвольного вектора $\mathbf{V} = (a, b, c, d)$ данной алгебры.

$$\forall \mathbf{V} = (a,b,c,d)\,\exists \mathbf{V}^{-1} \Leftrightarrow dc \neq ab \tag{3}$$

Таким образом, вектор $\mathbf{N} = (a,b,c,d)$ необратим тогда и только тогда, когда $dc = ab$.

После определения критерия необратимости следует определить множества левых и правых локальных единиц, соответствующих произвольному необратимому вектору. С учетом, что $dc = ab$, из системы (2) мы получаем множество левосторонних локальных единиц, координаты y и w которых задаются формулами (4) и (5), а координаты x и z являются произвольными элементами поля $GF(p)$.

$$w = \frac{a}{a\beta + c} - \frac{a + c\alpha}{a\beta + c}x, \tag{4}$$

$$y = \frac{c}{a\beta + c} - \frac{a + c\alpha}{a\beta + c}z, \tag{5}$$

Множество правых локальных единиц формируется аналогично. При этом множества левых и правых локальных единиц содержат как обратимые, так и необратимые вектора.

Новая форма скрытой ЗДЛ. В случае задания скрытой ЗДЛ, ориентированной на применение в алгоритме ЭЦП, имеется возможность более глубокой маскировки ЗДЛ, по сравнению со случаем разработки протоколов открытого распределения ключей и открытого шифрования. Действительно, в случае последних двух криптосхем требуется задать использование различными пользователями одной и той же циклической группы (скрытость ЗДЛ, связана с переводом значения открытого ключа в различные циклические группы путем выполнения операции сопряжения с секретным элементом сопряжения), тогда как в схеме ЭЦП каждый владелец открытого ключа может использовать уникальную скрытую циклическую группу.

Идея новых форм задания скрытой ЗДЛ, ориентированных на применение в схемах ЭЦП состоит в следующем. Выбрав некоторую скрытую циклическую группу, порядок которой равен достаточно большому простому числу, и некоторую известную схему ЭЦП, основанную на обычной ЗДЛ, пользователь формирует пару элементов НКАА связанных с элементами $\mathbf{N}$ и $\mathbf{N}^x$, где секретное значение $\mathbf{N}$ является генератором скрытой группы. Подпись вычисляется для случая явного использования выбранной схемы ЭЦП, а проверка подлинности подписи выполняется путем осуществления операций возведения в степень в двух различных циклических группах.

Для реализации этого принципа предлагаются следующая новая форма скрытой ЗДЛ, которая использует то, что в НКАА (рис. 1), для отдельных необратимых элементов алгебры имеется большое число локальных односторонних и двухсторонних единиц. Например, для элемента $\mathbf{N} = (a,b,c,d)$ при $dc = ab$ множество всех левосторонних локальных единиц описывается формулами (4) и (5). Зададим формирование личного секретного ключа подписанта в соответствии со следующей процедурой.

Процедура формирования личного секретного ключа.

Шаг 1. Выбрать простое число p большой разрядности (от 256 до 512 бит) в качестве характеристики поля $GF(p)$

Шаг 2. Сгенерировать случайный необратимый элемент $\mathbf{N}$, значение локального порядка которого равно простому числу q достаточно большой разрядности.

Шаг 3. Выбрать три случайных обратимых 4-мерных вектора $\mathbf{E}_1$, $\mathbf{E}_2$ и $\mathbf{E}_3$, координаты которых удовлетворяют формулам (4) и (5), т. е. из множества локальных левосторонних единиц, относящихся к элементу $\mathbf{N}$.

Шаг 4. Выбрать случайный обратимый вектор $\mathbf{G}$, такой, что имеет место неравенство $\mathbf{N} \circ \mathbf{G} \neq \mathbf{G} \circ \mathbf{N}$.

Шаг 5. Вычислить следующие обратимые элементы: $\mathbf{U} = \mathbf{E}_1 \circ \mathbf{G}^{-1}$, $\mathbf{H} = \mathbf{U}^{-1} \circ \mathbf{E}_2$, $\mathbf{T} = \mathbf{E}_3 \circ \mathbf{H}^{-1}$.

Шаг 6. Выбрать случайное число $x < q$.

Секретным ключом подписанта является натуральное число x и тройка 4-мерных векторов $\mathbf{N}$, $\mathbf{G}$ и $\mathbf{T}$. Все остальные значения, использованные в ходе выполнения процедуры формирования личного секретного ключа, также являются секретными. При этом они могут быть уничтожены после формирования открытого ключа подписанта, который вычисляется в виде следующей пары векторов $\mathbf{Y}$ и $\mathbf{Q}$ по формулам (6) и (7) соответственно.

$$\mathbf{Y} = \mathbf{G} \circ \mathbf{N}^x \circ \mathbf{U} \tag{6}$$

$$\mathbf{Q} = \mathbf{H} \circ \mathbf{N} \circ \mathbf{T} \tag{7}$$

Из формул (6) и (7) видно, что элементы открытого ключа $\mathbf{Y}$ и $\mathbf{Q}$ принадлежат различным циклическим группам, содержащимся в рассматриваемой алгебре как ее подмножества, но при этом векторы $\mathbf{Y}$ и $\mathbf{Q}$ связаны с одной и той же замаскированной циклической группой, генерируемой вектором $\mathbf{N}$. Скрытая ЗДЛ состоит в вычислении значения x по известным векторам $\mathbf{Y}$ и $\mathbf{Q}$, которые принадлежат разным циклическим группам, содержащихся в используемой КНАА.

Постквантовая схема цифровой подписи. На основе предложенной новой формы, скрытой ЗДЛ разработана схема ЭЦП, описываемая следующими процедурами генерации и проверки подлинности ЭЦП.

Процедура генерации ЭЦП.

Шаг 1. Выбрать случайное число $k < q$ и вычислить вектор $\mathbf{W} = \mathbf{G} \circ \mathbf{N}^k \circ \mathbf{T}$.

Шаг 2. Вычислить двоичное число $e = F_h(M, \mathbf{W})$ где F_h некоторая заранее заданная хэш-функция.

Шаг 3. Вычислить натуральное число $s = k + ex \bmod q$.

На вход процедуры генерации ЭЦП подается электронный документ M и секретный ключ подписанта $(x, \mathbf{N}, \mathbf{G}, \mathbf{T})$. Результатом работы процедуры является ЭЦП в виде пары чисел (e, s).

Процедура проверки подлинности ЭЦП.

Шаг 1. Вычислить вектор $\widetilde{\mathbf{W}} = \mathbf{Y}^{q-e} \circ \mathbf{Q}^s$.

Шаг 2. Вычислить двоичное число $\widetilde{e} = F_h(M, \widetilde{\mathbf{W}})$.

Шаг 3. Если $\widetilde{e} = e$ то признать подпись (e, s) подлинной. В противном случае отвергнуть подпись.

На вход процедуры проверки ЭЦП подается ЭЦП (e, s), документ M, открытый ключ $(\mathbf{Y}, \mathbf{Q})$. Результатом работы процедуры является сообщение о подлинности или ложности ЭЦП.

Формальное доказательство корректности работы схемы ЭЦП может быть выполнено путем подстановки значения ЭЦП (e, s), полученного на выходе процедуры генерации подписи, на вход процедуры проверки ее подлинности.

$$\widetilde{\mathbf{W}} = \mathbf{Y}^e \circ \mathbf{Q}^s = \left(\mathbf{G} \circ \mathbf{N}^x \circ \mathbf{U}\right)^{q-e} \circ \left(\mathbf{H} \circ \mathbf{N} \circ \mathbf{T}\right)^s = \mathbf{G} \circ \left(\mathbf{N}^x \circ \mathbf{E_1}\right)^{q-e-1} \circ \mathbf{N}^x \circ \mathbf{U} \circ \mathbf{H} \circ \left(\mathbf{N} \circ \mathbf{E}_3\right)^{s-1} \circ \mathbf{N} \circ \mathbf{T} =$$
$$= \mathbf{G} \circ \left(\mathbf{N}^x\right)^{q-e-1} \circ \mathbf{N}^x \circ \mathbf{E}_2 \circ \mathbf{N}^{s-1} \circ \mathbf{N} \circ \mathbf{T} = \mathbf{G} \circ \mathbf{N}^{eq-ex} \circ \mathbf{E_2} \circ \mathbf{N}^s \circ \mathbf{T} =$$
$$= \mathbf{G} \circ \mathbf{N}^{eq-ex+s} \circ \mathbf{T} = \mathbf{G} \circ \mathbf{N}^{eq-ex+(k+ex)} \circ \mathbf{T} = \mathbf{G} \circ \mathbf{N}^{eq} \circ \mathbf{N}^k \circ \mathbf{T} = \mathbf{G} \circ \mathbf{N}^k \circ \mathbf{T} =$$
$$= \mathbf{W} \Rightarrow \widetilde{e} = F_h\left(M, \widetilde{\mathbf{W}}\right) = F_h\left(M, \mathbf{W}\right) = e$$

Разработанная схема ЭЦП повторяет схему подписи Шнорра в скрытой циклической группе, генерируемой необратимым элементом $\mathbf{N}$. В ходе проверки подлинности ЭЦП выполняются операции возведения в большую степень над векторами $\mathbf{Y}$ и $\mathbf{Q}$, принадлежащими двум различным циклическим группам КНАА, поэтому для взлома схемы подписи потенциальному атакующему потребуется решать скрытую ЗДЛ. Использование необратимого вектора предотвращает гипотетические обобщенные атаки [14], основанные на нахождении гомоморфных отображения НКАА в поле $GF(p)$.

Заключение.

В качестве носителя скрытой ЗДЛ предложена новая 4-мерная НКАА, заданная над простым конечным полем, и описаны множества единичных элементов различного типа. В качестве примитива постквантовых схем ЭЦП предложена новая форма скрытой ЗДЛ. На основе последней построен протокол ЭЦП, реализующий маскируемую схему подписи Шнорра. Сравнение известной и предложенной форм скрытой ЗДЛ показывает, что первая обеспечивает более глубокое маскирование циклической группы, из которой выбираются два элемента, связанные операцией возведения в большую степень и используемые для вычисления открытого ключа. Новая форма скрытой ЗДЛ ориентирована на применение в качестве примитива протоколов ЭЦП и не может быть использована для построения протоколов открытого распределения ключей.

Разработанная схема ЭЦП представляет интерес как постквантовый примитив, поскольку она обладает достаточной высокой производительностью процедур генерации и проверки подлинности ЭЦП, малым размером подписи и сравнительно малым размером открытого ключа, позволяет подписать неограниченное число различных документов с использованием одного открытого ключа.

СПИСОК ЛИТЕРАТУРЫ

1. Menezes A.J., Van Oorschot P.C., and Vanstone S.A. Handbook of Applied Cryptography. – Boca Raton, FL: CRC Press, 1997. – 780 p.
2. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM Journal of Computing. 1997. Vol. 26. P. 1484–1509
3. Smolin J. A., Smith G., Vargo A. Oversimplifying quantum factoring // Nature. 2013. vol. 499, no. 7457. pp. 163–165.
4. Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings. // Lecture Notes in Computer Science series. Springer, 2018. Vol. 10786.
5. Proceedings of the 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016. Fukuoka, Japan, February 24-26, 2016 // Lecture Notes in Computer Science (LNCS) series. Springer, 2016. vol. 9606. - 270 p.
6. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. NIST PQCrypto project. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf
7. First NIST standardization conference - April 11--13, 2018. http://prometheuscrypt.gforge.inria.fr/2018-04-18.pqc2018.html
8. Moldovyan D.N. Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes // Quasigroups and Related Systems. 2010. Vol. 18. P. 165−176.
9. Каргаполов М. И., Мерзляков Ю.И. Основы теории групп. – М.: Физматлит, 1996. – 287 с.
10. Молдовян Н.А., Абросимов И.К., Ковалева И.В. Постквантовый протокол бесключевого шифрования // Вопросы защиты информации. 2017. № 3 (118). С. 3–13
11. Молдовян Д.Н., Куприянов А.И., Костина А.А., Захаров Д.В. Задание некоммутативных конечных групп векторов для синтеза алгоритмов цифровой подписи // Вопросы защиты информации. 2009. № 4. С. 13
12. Moldovyan D.N., Moldovyan N.A. Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms // Quasigroups and Related Systems. 2010. Vol. 18. P. 177-186
13. Глухов М.М. К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах // Математические вопросы криптографии. 2010 Т. 1 № 4 С. 5−22.
14. Молдовян Н.А., Moldovyanu P.A, Vector Form of the Finite Fields GF(pm) // Bulletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2009. No 3 (61). P. 57-63.

УДК 004

КРИТЕРИИ И ПОКАЗАТЕЛИ КЛАССИФИКАЦИИ ИНСАЙДЕРОВ

Поляничко Марк Александрович, Королев Александр Игоревич
Санкт-Петербургский государственный университет путей сообщения императора Александра I
Московский пр., 9, Санкт-Петербург, 190031, Россия
e-mails: polyanichko@pgups.ru, korolev@pgups.ru

Аннотация. Рассматривается проблема инсайдеров, как внутренней угрозы информационной безопасности и предлагаются критерии классификация инсайдеров. Предлагаемые критерии описывают инсайдера по различным параметрам, в том числе параметрам, характеризующим его трудовые отношения с организацией, уровень профессиональной подготовки и мотивацию. Для анализа возможных инсайдерских угроз, представлены показатели риска: личностного, поведенческого и технического.

Ключевые слова: внутренние угрозы информационной безопасности; инсайдер; обнаружение инсайдеров.

CRITERIA AND INDICATORS FOR CLASSIFYING INSIDERS

Polyanichko Mark, Korolev Alexander
Emperor Alexander I St. Petersburg State Transport University
9 Moskovsky Av., St. Petersburg, 190031, Russia
e-mails: polyanichko@pgups.ru, korolev@pgups.ru

Abstract. Considers the problem of insiders as an internal threat to information security and suggests criteria for classifying insiders. The proposed criteria describe the insider by various parameters, including parameters characterizing his labor relations with the organization, personal characteristics and motivation. Proposed risk indicators for insider threat analysis: personal, behavioral and technical.

Keywords: internal threats to information security; insider; detection of insiders.

Инсайдерские угрозы — это угрозы, которые исходят от людей внутри организации (работников, бывших работников, подрядчиков или деловых партнеров), у которых есть информация о наличии ценных данных в организации, методах обеспечения безопасности и информационных системах, использующихся в организации. Угроза данного вида может включать мошенничество, кражу конфиденциальной и коммерчески ценной информации, воровство интеллектуальной собственности или саботаж работы информационных систем. Растущая зависимость организаций от информационной инфраструктуры, технологий и информационных активов в условиях широкой доступности инструментов для злоумышленников свидетельствует о том, что проблема инсайдеров будет приобретать всё большую актуальность.

Разработка методов обнаружения нереализуема в условиях отсутствия классификации инсайдеров как внутренней угрозы информационной безопасности. Для решения данной задачи приведена классификация инсайдеров по различным критериям, в том числе характеризующим его трудовые отношения с организацией, уровень профессиональной подготовки и мотивацию.

Классификация по местоположению

Инсайдер может быть классифицирован по местоположению в пространстве. Можно различать физическое и логическое присутствие инсайдера в организации. Данная классификация так же является темпоральной, так как в разные моменты времени, один и тот же инсайдер может представлять, как внутреннюю, так и внешнюю угрозу. Под логическим присутствием в данной классификации понимается факт его авторизации.

Классификация по намерению

Для классификации инсайдеров по виду действий предлагается деление видов действий по намерению на случайные и преднамеренные.

Классификация по видимости действий

Классификация по видимости действий подразумевает деление инсайдеров на два вида: на инсайдеров, скрывающих свои действия и инсайдеров, действующих открыто.

Классификация по наличию плана действий

Различаются инсайдеры, действующие спонтанно и инсайдеры, действующие на основании плана. При этом план работ может быть сформирован как самим инсайдером, так и третьей заинтересованной стороной.

Классификация по источнику мотивации

Инсайдеры должны быть мотивированы для совершения неправомерных действий. Источники мотивации можно разделить на внутренние и внешние. К внутренним источникам мотивации можно отнести скуку, амбиции, раздражение, зависть. К внешним источникам мотивации можно отнести долги, финансовые проблемы, шантаж, увольнение, подкуп и т.д [1].

Классификация по уровню подготовки

Классифицируются как имеющие ИТ подготовку и не имеющие ИТ подготовку. Инсайдеры могут относиться к числу ИТ специалистов организации. Наличие определенных навыков у инсайдера может серьезно затруднить процесс его обнаружения, а в ряде случаев сделать обнаружение невозможным.

Классификация по взаимоотношению с организацией

Инсайдеры могут быть классифицированы по трудовым взаимоотношениям с организацией: сотрудник, имеющий действующее штатное трудоустройство, уволенный сотрудник, сотрудник, работающий по договору, лицо, аффилированное с штатным сотрудником (сотрудником, работающим по договору).

Классификация по уровню доступа

Привилегированные и непривилегированные. Данная классификация делит инсайдеров по признаку наличия доступа к конфиденциальной или другой критичной информации. Чем выше уровень доступа инсайдера, тем больший ущерб он может нанеси организации.

В свою очередь, для моделирования вредоносной инсайдерской угрозы необходимо основываться на трех показателях риска: личностных, поведенческих и технических [2].

Личностные показатели риска

Индивидуальные черты характера отдельных людей довольно стабильны и не изменяются в течение жизни. Обнаружение статистически значимой связи между различными профилями личности может служить основой для разработки и внедрения протоколов безопасности, учитывающих специфические личностные характеристики работников.

Поведенческие показатели риска

Важным аспектом теории запланированного поведения является то, что, люди должны придерживаться определенного шаблона поведения, но, на практике, намерения могут измениться при появлении новых обстоятельств. Поведенческие теории определяют основные принципы того, как на различных этапах поведение инсайдера проявляется через определенные показатели. Теория запланированного поведения предполагает, что намерения человека, его отношение к преступлению и этические нормы являются ключевыми факторами при прогнозировании поведения. Проверка данных до трудоустройства, может помочь определить людей, имеющих поведенческие показатели риска и склонных к инсайдерскому поведению. Многие факторы риска, могут быть не связаны с трудовой деятельностью и могут быть вызваны фобиями, проблемами в личной жизни, долгами или иными причинами.

Технические показатели риска

Имеется шесть видов данных, получаемых из систем журналирования, которые могут быть использованы для обнаружения подозрительных действий. К ним относятся данные об аутентификации, изменение данных, сетевая активность, получение доступа к ресурсам, активность вредоносного программного обеспечения и системные ошибки. Программные средства защиты информации, такие как SIEM и IDS/IPS системы могут быть использованы для предоставления администраторам достаточной информации для обнаружения подозрительной активности. Изменения в конфигурационных файлах, получение доступа к журналам авторизации могут быть анализированы для наблюдения за активностью сотрудников. Таким образом, в случае, если обнаружено необычное поведение, отличное от профиля поведения нормального поведения, то может быть сделано предположение об инсайдерской деятельности.

Приведенная классификация отражает различные существенные стороны поведения инсайдеров. Так как различные виды инсайдерского поведения требуют различных методов обнаружения и реагирования, данная классификация может быть использована при создании методов и методик обнаружения внутренних угроз информационной безопасности. Также данная классификация может быть использована для оценки рисков от внутренних угроз информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Анализ угроз информационной безопасности 2016-2017 // [сайт] URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Analysis_infor-mation_security_threats_2016_2017.
2. Fagade T., Spyridopoulos T., Albishry N., Tryfonas T. (2017) System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis. In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science, vol 10292. Springer, Cham

УДК 004.052.3

МЕТОДИКА ОПРЕДЕЛЕНИЯ НАДЕЖНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Садикова Анастасия Александровна, Кузнецов Александр Юрьевич, Жарков Арсений Дмитриевич
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: anastasiiasad1004@gmail.com, al.ur.kouznetsov@gmail.com, arsenzhar@gmail.com

Аннотация. При проектировании автоматизированной информационной системы в защищенном исполнении предполагается интегральный подход к организации системы защиты информации, в связи с этим в комплекс мер и средств защиты входят организационные, программные, программно-аппаратные, инженерно-технические. Поскольку при эксплуатации автоматизированной информационной системы в защищенном исполнении и поддержании ее системы защиты информации задействован персонал, то система также является эргатической. Выбранные средства и меры, предназначенные для защиты ценных информационных ресурсов, могут содержать в себе ошибки, недоработки, а также различные закладные устройства. По этой причине

злоумышленник может воспользоваться этими уязвимостями и получить доступ к защищаемой информации. Для того чтобы оценить, насколько та или иная система защиты способна выполнять предъявляемые к ней требования, необходимо рассчитать надежность ее функционирования. В статье проанализированы существующие модели надежности защиты информации, выявлены их достоинства и недостатки.

Ключевые слова: автоматизированная информационная система в защищенном исполнении; оценка надежности; теория надежности; защита информации.

THE METHOD OF DETERMINING THE RELIABILITY OF INFORMATION PROTECTION IN AN AUTOMATED INFORMATION SYSTEM IN SECURED EXECUTION

Sadikova Anastasiia, Kuznetsov Aleksandr, Zharkov Arseniy
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics
(University ITMO)
49 Kronverksky Av., St. Petersburg, 197101, Russia
e-mails: anastasiiasad1004@gmail.com, al.ur.kouznetsov@gmail.com, arsenzhar@gmail.com

Abstract. When designing an automated information system in a protected design, an integrated approach to the organization of an information security system is proposed; in this connection, the complex of measures and means of protection includes organizational, software, software, hardware, engineering and technical. Since the operation of the automated information system in protected execution and maintenance of its information security system involves personnel, the system is also ergatic. The chosen means and measures designed to protect valuable information resources may contain errors, defects, as well as various mortgage devices. For this reason, an attacker can exploit these vulnerabilities and gain access to protected information. In order to assess whether a particular protection system is capable of meeting the requirements to it, it is necessary to calculate the reliability of its functioning. The article analyzes the existing methods for determining the reliability of information security, reveals their advantages and disadvantages.

Keywords: automated information system in secured execution; reliability assessment; reliability theory; protection of information.

Введение.

После создания системы защиты информации (СЗИ) на предприятии или ее проекта возникают вопросы оценки надежности СЗИ и времени преодоления системы защиты злоумышленником. Создание СЗИ осуществляется в три этапа. На первом этапе разрабатывается базовая модель системы, которая будет функционировать в компании. Второй этап включает разработку системы защиты. Третий, завершающий этап – это поддержка работоспособности системы, регулярный контроль и управление рисками. Важно, чтобы модуль защиты отличался гибкостью и позволял администратору безопасности быстро совершенствовать систему при обнаружении новых потенциальных угроз. При проектировании СЗИ необходимо учитывать, что защита информации должна быть постоянной, целевой, плановой (соответствует требованиям нормативно-правовых актов), активной, комплексной, универсальной (средства защиты информации выбираются в соответствии с обнаруженными утечками) и надежной.

Надежность СЗИ – характеристика способности программного, аппаратного, аппаратно-программного средства выполнить при определенных условиях требуемые функции в течение определенного периода времени.

В данной работе будут проанализированы модели надежности СЗИ.

Управление надежностью систем защиты информации как метод обеспечения защищенности информационных ресурсов (С. К. Варлатая)

В данной работе авторы описывают модель надежности СЗИ последовательно-параллельными соединениями элементов защиты. По истечении промежутка времени, в течении которого СЗИ функционирует в бесперебойном режиме, происходит возможный отказ системы, т.е. событие, вследствие которого СЗИ не может выполнить возложенные на него функции. Таким образом, надежность в данной работе синонимична с понятием «отказоустойчивость».

Для расчета надежности системы авторы предлагают декомпозировать ее на отдельные блоки (логически или технически цельные) и производить расчет уже отдельно для каждого блока и соединения (последовательного и/или параллельного). Отмечено, что при параллельном соединении элементов отказоустойчивость системы выше, чем при последовательном. Это связано с тем, что в последнем случае при отказе одного элемента защиты, происходит отказ всей СЗИ. Отказ системы при параллельном соединении наступает только в случае одновременного отказа всех элементов системы.

Также при расчете надежности СЗИ необходимо учитывать такой параметр, как интенсивность отказов, т.е. число отказов на единицу времени по отношению к общему количеству элементов системы. Нормальная эксплуатация элементов СЗИ подразумевает, что интенсивность отказов является постоянной величиной. Таким образом, вероятность безотказной работы элемента СЗИ в соответствии с его экспоненциальной моделью надежности можно найти по формуле (1).

$$P(t) = e^{-\lambda t}, \quad (1)$$

где λ – интенсивность отказов, t – время.

При комплексной защите информации итоговая СЗИ становится смешанной, т.е. система с параллельно-последовательным соединением элементов. Для расчета надежности такой СЗИ необходимо воспользоваться формулой (2).

$$P_{\text{СЗИ}} = 1 - \prod_i^n (1 - e^{-t\sum_{k=1}^{m}\lambda_k}), \quad (2)$$

где n – количество параллельно соединенных блоков элементов СЗИ, m – количество последовательно соединенных элементов СЗИ.

Из графика данной функции видно, что надежность смешанной СЗИ зависит от времени. Причем существует три временных интервала: на первом промежутке отмечено слабое убывание функции надежности; на втором происходит резкое падение надежности; на третьем интервале надежность становится практически постоянной величиной и для данного графика она минимальна. Отмечено, что интенсивность отказов напрямую влияет на длину первого интервала, на котором надежность СЗИ максимальна [1].

Авторами статьи предлагается установить минимально достаточный уровень надежности СЗИ, при котором суммарный риск защищаемой информации находится в пределах нормы. Основываясь на знаниях значений интенсивности отказов для каждого элемента СЗИ (установлены производителем), следует определить временной период наиболее устойчивого функционирования СЗИ. В течение него необходимо проводить различные профилактические работы, направленные на поддержание СЗИ в эффективном состоянии.

Недостатком этого метода является проблема декомпозиции и четкого выделения элементов СЗИ. Также требуется детализация моделей надежности отдельных компонентов СЗИ.

Принципы построения модели надежности системы защиты информации. (О. М. Булгаков)

Авторы данной работы так же при описании модели надежности системы опираются на тип соединения элементов защиты (последовательное и/или параллельное). Однако, преимуществом этой модели перед предыдущей является классификация средств и мер защиты информации, применяемых для обеспечения безопасности охраняемого объекта, а именно: организационные меры; инженерно-технические средства; программные средства; физические (эргатические) средства. В свою очередь эти компоненты соединены параллельно. Каждый блок элементов может функционировать вне зависимости от работоспособности других, обеспечивая некоторый уровень защиты.

Вероятность безотказной работы СЗИ определяется по формуле (3).

$$P = 1 - P_{\text{отк}} = 1 - P_{\text{О}} \cdot P_{\text{Т}} \cdot P_{\text{П}} \cdot P_{\text{Ф}}, \quad (3)$$

где $P_{\text{отк}}$ – вероятность отказа СЗИ; $P_{\text{О}}, P_{\text{Т}}, P_{\text{П}}, P_{\text{Ф}}$ – вероятности отказа соответственно организационных, инженерно-технических, программных и физических компонентов СЗИ.

В случае СЗИ отказ понимается как возникновение уязвимости, возможности преодоления СЗИ злоумышленником. В работе рассмотрены причины и механизмы отказов отдельных компонентов СЗИ [3].

Оценка надежности систем защиты информации (А. А. Пономорёв)

В работе автора получена модель СЗИ, которая позволяет вычислять среднее время преодоления СЗИ злоумышленником, используя аппарат теории массового обслуживания (ТМО). Модель разработана на основе теории Марковских цепей. Выделяется два фактора, влияющие на надежность СЗИ: отказы технических и программных средств, обеспечивающих защиту информации; нахождение злоумышленником уязвимостей в СЗИ.

Анализируемая СЗИ рассматривается как система массового обслуживания с состояниями, полученными изменением трех признаков: система не уязвима (уязвимости не известны) или система с известной уязвимостью; СЗИ работоспособна или отказ системы; есть попытка НСД или нет. Считается, что вероятность изменения состояния сразу по двум признакам пренебрежимо мала. Таким образом, для рассматриваемой системы характерно 9 состояний. Последнее девятое состояние является возвратным (поглощающим) и характеризует состояние получения злоумышленником интересующей его информации. Для дальнейшего исследования данное состояние исключается и рассматриваются только невозвратные [3].

Среднее время пребывания СЗИ во множестве невозвратных состояний рассчитывается по формуле (4) и отражает надежность системы, количество времени которое система будет выполнять свои функции.

$$t = P^{(0)1}\Gamma, \quad (4)$$

где $P^{(0)1}$ – вектор начального распределения; $\Gamma = N\text{E}$, где $N = (1 - \text{Q})^{-1}$ – фундаментальная матрица поглощающей Марковской цепи (Q – матрица переходов из состояния в состояние), E – суммирующий вектор-столбец.

Данная модель позволяет сравнивать различные СЗИ между собой, а также разрабатывать СЗИ с заданным временем преодоления.

Заключение.

В работе проанализированы некоторые модели надежности СЗИ. Стоит отметить, что при выборе средств защиты информации следует использовать сертифицированные средства, поскольку в таком случае риск утечки информации через закладное устройство в самом средстве защиты становится минимальным. Также необходимо следить за актуальностью нормативных правовых актов, по которым работает организация, должностных инструкций сотрудников, систем руководящих документов и документов, регламентирующих ее работу. Следует заменить морально и физически устаревшие средства защиты, а также обновить средства в случае, если возможности текущего оборудования не соответствуют задачам системы защиты в настоящее время.

СПИСОК ЛИТЕРАТУРЫ

1. Варлатая С. К., Урзов А. Ю. Управление надежностью систем защиты информации как метод обеспечения защищенности информационных ресурсов (Актуальные вопросы технических наук в современных условиях, / Сборник научных трудов по итогам международной научно-практической конференции. № 3. г.Санкт-Петербург, 2016. 151 с.)
2. Булгаков О. М., Удалов В. П., Кучмасов Е. А. Принципы построения модели надежности системы защиты информации // Вестник ВИ МВД России. — 2012. — № 3. — С. 167–176.
3. Пономарев А.А. Оценка надежности систем защиты информации // REDS: Телекоммуникационные устройства и системы. 2014. №4. С. 431-432.

УДК 004.942: 621.373.54

ИССЛЕДОВАНИЕ ФОРМИРОВАНИЯ БИПОЛЯРНЫХ СВЕРХКОРОТКИХ ИМПУЛЬСОВ НАПРЯЖЕНИЯ БОЛЬШОЙ МОЩНОСТИ НА ОСНОВЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Сорокин Леонид Николаевич, Усыченко Алексей Сергеевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14 линия 39, Санкт-Петербург, 199178, Россия
e-mails: sorokinln@mail.ru, a.usychenko@gmail.com

Аннотация. Разработаны компьютерные модели в среде CST Studio Suite, реализующие два способа формирования биполярных импульсов сверхкороткой длительности большой мощности, состоящих в наложении униполярных импульсов противоположной полярности смещенных относительно друг друга во времени с использованием длинных линий. Подробно исследован процесс формирования биполярных импульсов обоими способами. Показано преимущество в энергетической эффективности преобразования одного способа над другим.

Ключевые слова: сверхкороткий импульс; генератор униполярных импульсов напряжения; биполярный импульс; компьютерная модель; длинная линия; имитационное моделирование.

STUDY OF THE FORMATION OF BIPOLAR ULTRA-SHORT VOLTAGE PULSES OF HIGH POWER ON THE BASIS OF SIMULATION

Sorokin Leonid, Usychenko Aleksey
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th Line St, Petersburg, 199178, Russia
e-mails: sorokinln@mail.ru, a.usychenko@gmail.com

Abstract. Computer models have been developed in the CST Studio Suite environment that implement two methods of generating bipolar pulses of ultrashort duration of high power, consisting in imposing unipolar pulses of opposite polarity shifted relative to each other in time using long-lines. The process of the formation of bipolar pulses by both methods is investigated in detail. The advantage in the energy efficiency of converting one method over another is shown.

Keywords: bipolar impulse; ultrashort impulse of high power; generator of voltage unipolar impulses; computer model; long line; simulation.

Введение. В настоящее время актуальной научно-технической задачей является создание мощных излучателей сверхкоротких электромагнитных импульсов (ЭМИ) на основе твердотельных генераторов большой мощности и сверхширокополосных антенн. Такие излучатели широко применяются в различных областях прикладной науки и техники [1-3], в частности, в специальной радиотехнике [4-5].

Большинство создаваемых твердотельных генераторов формируют униполярные импульсы напряжения большой мощности, неизменной формы и длительности [6], каждый из которых имеет свой уникальный энергетический спектр. Поэтому для каждого такого сверхкороткого импульса (СКИ) подбирается энергетически оптимальная сверхширокополосная антенна с такой центральной частотой f_c и полосой пропускания Δf, в которую попадает максимально возможное количество энергии СКИ. Особенность таких генераторов состоит в том, что изменение одного из параметров генерируемого импульса, например, формы всегда приводит к изменению другого параметра – его длительности и наоборот. Энергетический спектр генерируемого импульса при этом меняется и антенна, как правило, перестает быть энергетически оптимальной.

Униполярные импульсы излучаются сверхширокополосными антеннами менее эффективно, чем биполярные импульсы [1]. Однако твердотельные генераторы биполярных импульсов являются маломощными [7]. Амплитуды генерируемых ими импульсов напряжения составляют десятки-сотни вольт, что на 3…4 порядка меньше, чем у генераторов униполярных импульсов. С практической точки зрения важно знать, насколько эффективно применение генераторов тех или иных типов.

В настоящей работе на основе имитационного моделирования в среде CST Studio Suite решается задача оценивания энергетической эффективности преобразования униполярных импульсов в биполярные импульсы различными способами с использованием линий с распределёнными параметрами («длинных линий») [8].

Моделирование трансформации униполярных импульсов. В общем случае возможны два способа формирования биполярных импульсов из униполярных, состоящих в наложении двух импульсов

противоположной полярности, сопоставимой длительности и амплитуды, смещенных относительно друг друга во времени [1].

В первом способе (рис. 1«а») полагается, что биполярный импульс формируется одним генератором униполярных импульсов. Во втором способе, биполярный импульс формируется двумя генераторами униполярных импульсов разной полярности (рис. 1«б»). В обоих способах, форма формируемого биполярного импульса сильно зависит от геометрической длины L и волнового сопротивления Z длинных линий.

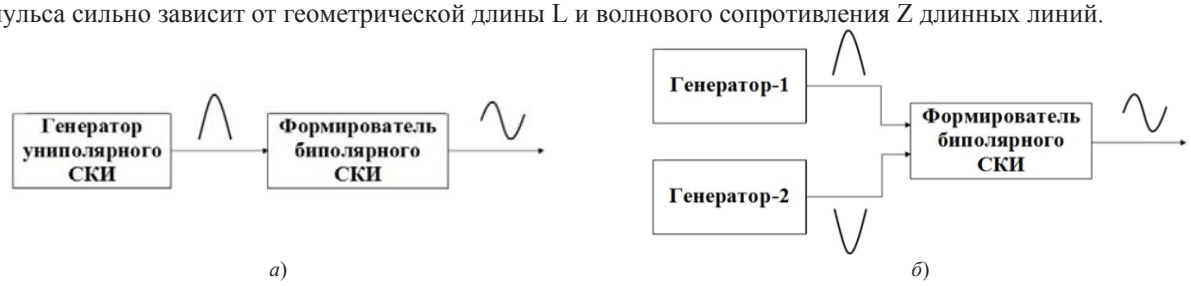


Рис. 1 – Способы формирования биполярных импульсов

В настоящей работе описанные способы реализованы в виде компьютерных моделей в среде моделирования и оптимизации трехмерных электромагнитных систем CST Studio Suite. Модель-1 реализует первый способ, при котором биполярный импульс на выходе модели создается за счет наложения импульса, формируемого самим генератором **Г** (падающего импульса) и импульса, отраженного от короткозамкнутого отрезка длинной линии. Модель-2 реализует второй способ, при котором биполярный импульс образуется посредством сложения двух импульсов противоположной полярности, формируемых разными генераторами **Г1** и **Г2** (см. ниже).

Структура и параметры разработанных моделей формирователей биполярных импульсов представлены на рис. 2.

В моделях использовались идеальные отрезки длинных линий. В процессе моделирования в каждой модели варьировали только двумя параметрами лишь одной линии (Линия-3) – её волновым сопротивлением Z и геометрической длиной L. Параметры двух других линий (Линия-1 и Линия-2) оставались постоянными величинами $Z_1 = Z_2 = 50$ Ом и $L_1 = L_2 = 100$ мм.

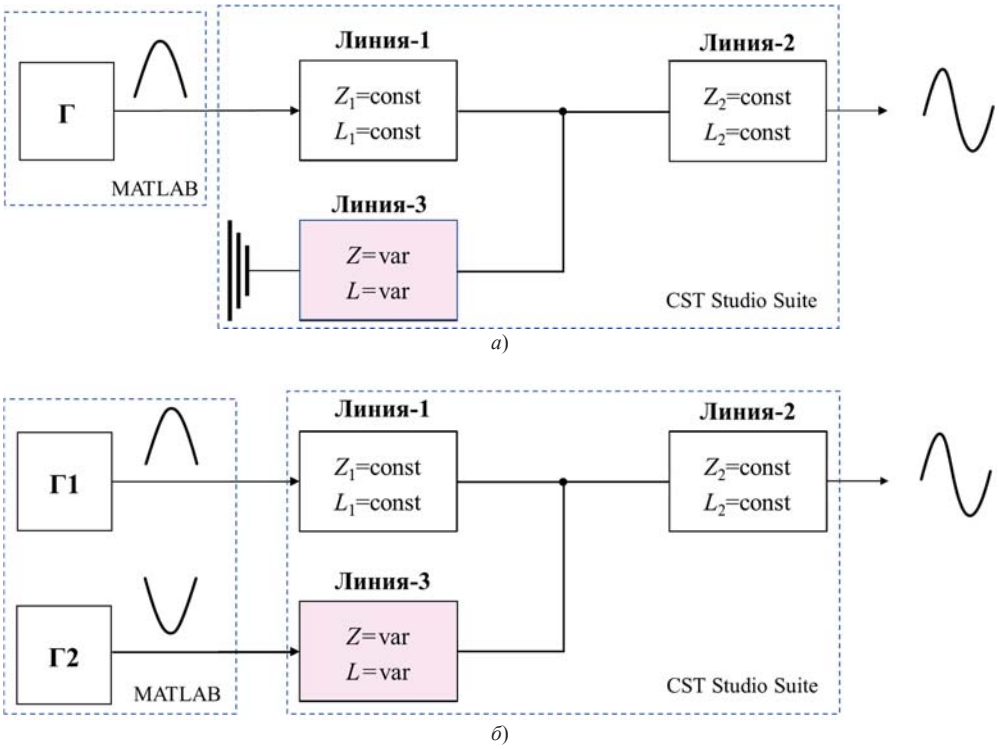
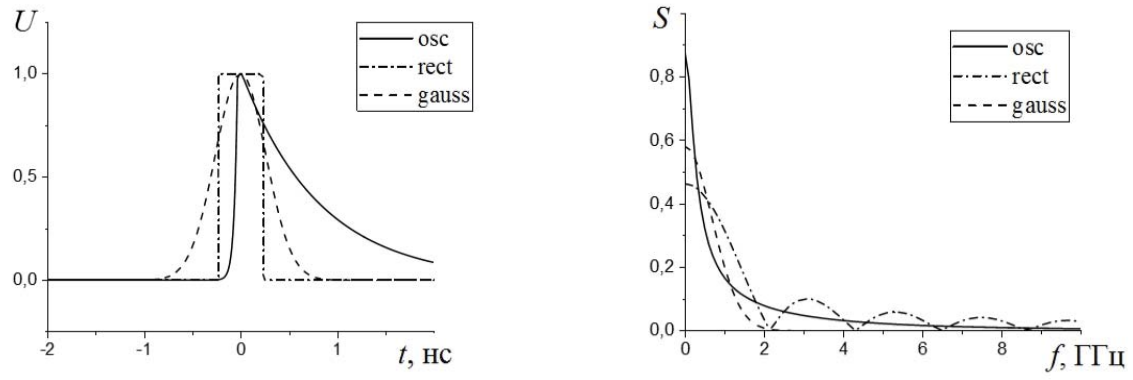


Рис. 2 – Структура и параметры разработанных моделей формирователей биполярных импульсов: модель-1 (*а*) и модель-2 (*б*)

Моделирование проводилось для трех форм униполярных импульсов напряжения $U(t)$ единичной амплитуды и одинаковой энергии W, содержащейся в каждом импульсе: осцилляторного импульса, гауссова импульса и прямоугольного импульса. На рис. 3«*а*» изображены формы этих импульсов, а на рис. 3«*б*» – модули их амплитудных спектров $S_U(f)$.



а) *б*)

Рис. 3 – Формы (*а*) униполярных импульсов и их амплитудные спектры (*б*)

Процедура расчёта и алгоритм моделирования. В процессе моделирования по аналогии с процедурой, описанной в работе [9], определяли энергию W_{uni} униполярного импульса и энергию W_{bi} сформированного биполярного импульса по формуле

$$W = \frac{2}{Z}\int_0^{\infty} S_U{}^2(f)\,df\,, \tag{1}$$

а также относительную долю δW энергии как отношение энергий этих импульсов

$$\delta W = \frac{W_{bi}}{W_{uni}}\,. \tag{2}$$

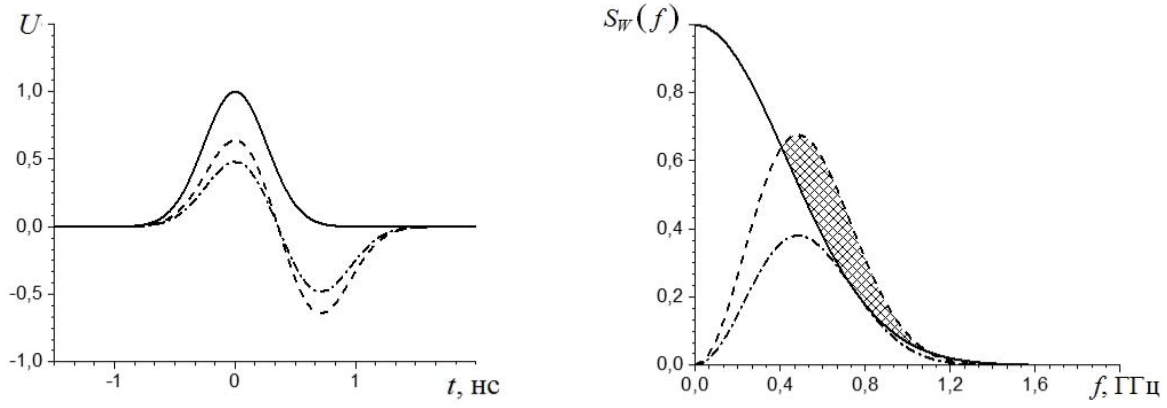
Энергетически эффективным считалось такое преобразование униполярных импульсов в биполярный импульс, при котором для выбранных значений Z и L относительная доля энергии δW достигает максимального значения $\delta W_{\max}$. При этом полученный таким образом биполярный импульс должен иметь симметричную форму положительной и отрицательной полуволн, чтобы в его энергетическом спектре отсутствовала постоянная составляющая и содержался единственный ярко выраженный экстремум $S_{W\max}$.

Процесс моделирования в среде CST Studio Suite был автоматизирован с помощью COM-интерфейса из среды MATLAB, где описанная выше процедура расчета реализована в виде программы. В программе использовалась встроенная функция оптимизации fminsearch, которая позволяла подбирать такие оптимальные значения параметров длинной линии (Линии-3) Z_{opt} и L_{opt}, при которых отношение (2) с учетом перечисленных условий достигает максимального значения $\delta W_{\max}$.

Результаты моделирования. На рис. 4 представлены результаты моделирования обоими способами для импульса гауссовой формы, удовлетворяющие всем изложенным выше требованиям. Условию $\delta W = \delta W_{\max}$ в этом расчете соответствуют оптимальные значения параметров Линии-3 $Z_{opt} = 50$ Ом и $L_{opt} = 125$ мм. На графике слева (рис. 4«а») изображены формы исходного униполярного импульса и полученные первым и вторым способами биполярные импульсы, а на графике справа (рис. 4«б») – их энергетические спектры $S_W(f)$.

Из этих графиков видно, что первый способ преобразования (когда имеется один генератор и короткозамкнутая линия) энергетически не эффективен. Энергия биполярного импульса, полученного этим способом, всегда меньше (примерно в 2 раза) энергии исходного импульса во всей полосе частот, а относительная доля энергии всегда меньше единицы ($\delta W < 1$).

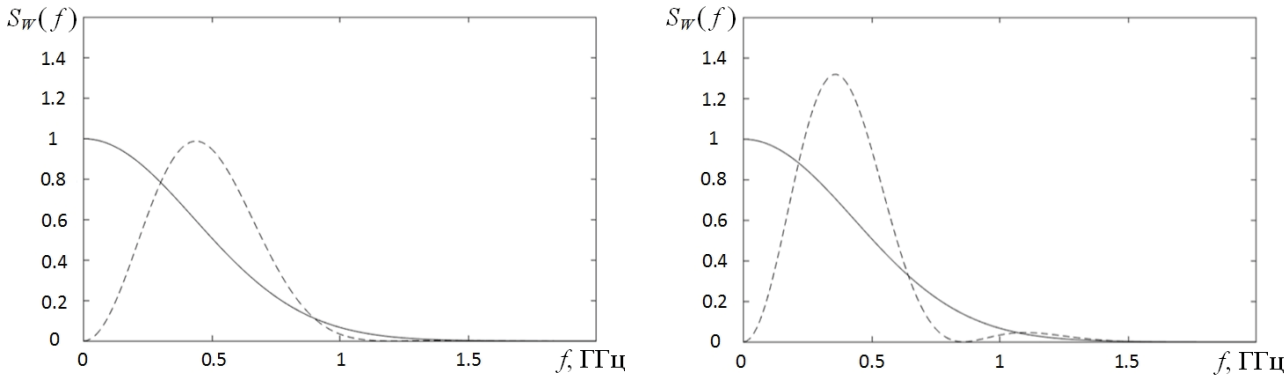
Второй способ преобразования (когда имеется два генератора) – энергетически эффективен, но не во всей полосе частот. Существует такая частота $f_{\text{гр}}$, выше которой энергия, содержащаяся в биполярном импульсе, оказывается больше энергии исходного униполярного импульса и относительная доля энергии $\delta W(f \geq f_{\text{гр}}) > 1$. Поэтому второй способ энергетически эффективен на частотах выше этой граничной частоты. Из рисунка 4«б» также видно, что во всей полосе частот сформированный биполярный импульс содержит $\delta W \approx 0{,}75$ от энергии W_{uni} исходного униполярного импульса, а на частотах $f \geq f_{\text{гр}}$ в нем содержится примерно на 50% больше энергии, чем у исходного униполярного импульса, и относительная доля энергии достигает значения $\delta W(f \geq f_{\text{гр}}) \approx 1{,}5$.



а) *б*)

Рис. 4 – Формы (*а*) униполярного импульса (*сплошная кривая*) и биполярных импульсов, рассчитанных в модели-1 (*штрихпунктирная кривая*) и модели-2 (*пунктирная кривая*), и их энергетические спектры (*б*) при $Z_{opt} = 50$ Ом и $L_{opt} = 125$ мм

Если изменить волновое сопротивление Линии-2, взяв, к примеру, $Z_2 = 0{,}5Z_1$, то можно получить и более энергетически выгодное решение, что видно из результатов, приведённых на рис. 5. В этом случае при $L_{opt} = 125$ мм относительная доля энергии (2) составит $\delta W \approx 0{,}92$ для всей полосы частот и $\delta W\left(f \geq f_{\text{гр}}\right) \approx 1{,}59$ на частотах $f \geq f_{\text{гр}}$ (см. рис. 5«*а*»), а при $L_{opt} = 135$ мм, соответственно: $\delta W \approx 0{,}99$ и $\delta W\left(f \geq f_{\text{гр}}\right) \approx 1{,}61$ (см. рис. 5«*б*»). Спектр сформированного биполярного импульса при этом становится более узким, что видно из сравнения рисунков 4«б», 5«а» и 5«б».



а) *б*)

Рис. 5 – Примеры форм энергетических спектров униполярного импульса (*сплошная кривая*) и биполярного импульса (*пунктирная кривая*), полученных вторым способом при $L_{opt} = 125$ мм (*а*) и $L_{opt} = 135$ мм (*б*)

В принципе для второго способа условие $\delta W \approx 1$ может выполняться не только на частотах $f \geq f_{\text{гр}}$, но и во всей полосе частот. Однако, в этом случае спектр имеет неравномерный вид и может содержать два и более локальных экстремума.

Следует также отметить, что существует множество значений параметров Линии-1, Линии-2 и Линии-3, для которых условие энергетической эффективности может соблюдаться в той или иной мере. Но не все они могут быть физически реализованы.

Всё выше сказанное справедливо и для других форм униполярных импульсов: осцилляторного и прямоугольного.

Заключение. Таким образом, установлено, что из двух известных способов формирования биполярного импульса из униполярного(-ных) энергетически эффективным является способ, основанный на применении двух генераторов униполярных импульсов.

Применение разработанной модели-2 на ранних этапах проектирования излучателей специального назначения позволяет, задавая форму и длительность униполярного импульса каждого генератора и подбирая параметры длинной линии, научно-обоснованно задавать требования к формирователям биполярных СКИ напряжения большой мощности с оптимальными спектральными и энергетическими характеристиками в требуемой полосе частот.

В перспективе все эти результаты позволят решить более общую задачу разработки энергетически-эффективных излучателей ЭМИ сверхкороткой длительности большой мощности с использованием оптимально-подобранных сверхширокополосных антенн под сформированный биполярный импульс.

СПИСОК ЛИТЕРАТУРЫ

1. Месяц Г.А., Яландин М.И. Пикосекундная электроника больших мощностей // Успехи физических наук. 2005. Т. 175. № 3. С. 225–246.
2. Сахаров К.Ю. Излучатели сверхкоротких электромагнитных импульсов и методы измерений их параметров. М.: Московский государственный институт электроники и математики. 2006. 159с.
3. Усыченко В.Г., Сорокин Л.Н. Стойкость сверхвысокочастотных радиоприемных устройств к электромагнитным воздействиям. Монография. – М.: Радиотехника, 2017. – 288 с.: 16 с. цв. ил.
4. Меркулов В.И., Сузанский Д.Н., Чернов В.С. Перспективы применения сверхкоротких импульсных сигналов в авиационных бортовых радиолокационных системах // Антенны. 2014. Выпуск 10(209). С. 11–19.
5. Слюсар В. Генераторы супермощных электромагнитных импульсов в информационных войнах // Электроника: наука, технология, бизнес. 2002. №5. С.60-67.
6. http://www.fidtechnology.com/products.html
1. 7 http://trimcom.ru/publications
7. Фуско В. СВЧ цепи. Анализ и автоматизированное проектирование: Пер. с англ. / Под ред. В.И. Вольмана. – М.: Радио и связь, 1990. – 288 с.: ил.
8. Усыченко В.Г., Усыченко А.С., Сорокин Л.Н. Энергетические характеристики излучателей сверхкоротких электромагнитных импульсов / Известия вузов. Радиофизика. 2015. Т.58. №2. – С.114 - 122.

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ И ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 004.056

ИСТОЧНИКИ УГРОЗ И ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Бобонец Сергей Алексеевич, Костюк Анатолий Владимирович
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: sbobon@mail.ru, kostyuk.anatoliy.2015@mail.ru

Аннотация. Рассматриваются актуальные задачи, стоящие перед обществом в период его информатизации, выделяются возникающие угрозы и проблемы информационно-психологической безопасности личности в условиях накопления и бесконтрольного распространения информационных ресурсов. Выделяются и анализируются два подхода к пониманию и обеспечению информационно-психологической безопасности личности. Формулируются задачи информационного и психологического образования в сфере информационно-психологической безопасности личности, позволяющие частичное решение отмеченных проблем.

Ключевые слова*:* угрозы; информационно-психологическая безопасность личности; подходы к пониманию и обеспечению информационно-психологической безопасности личности; информационное и психологическое образование.

SOURCES OF THREATS AND PECULIARITIES OF SECURITY INFORMATION SECURITY PERSONALITY

Bobonets Sergey, Kostyuk Anatoliy
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mails: sbobon@mail.ru, kostyuk.anatoliy.2015@mail.ru

Abstract. The current tasks facing the society in the period of its informatization are considered, emerging threats and problems of the information-psychological security of the individual in the conditions of accumulation and uncontrolled distribution of information resources are highlighted. Two approaches to understanding and ensuring information and psychological security of the individual are identified and analyzed. The tasks of informational and psychological education in the field of information-psychological security of a person are formulated, allowing partial solution of the problems noted.

Keywords*:* threats, information-psychological security of a person; approaches to understanding and ensuring information-psychological security of a person; information and psychological education.

Необходимо подчеркнуть, что одной из важнейших тенденций формирования современного общества становится его информатизация, которая проявляется в последовательной и систематической разработке и внедрении информационных технологий и информационных средств во все области деятельности человека. В современных условиях информация и информационные ресурсы выполняют важнейшую роль в развитии личности, общества и государства. Отмеченные особенности позволяют утверждать, что информатизация деятельности человека выступает в роли локомотива, ускоряющего развитие человечества и, что это развитие приближает страну к развитому информационному обществу [1].

Одной из актуальных задач, стоящих перед информационным обществом, является обеспечение его информационной безопасности. Решение данной задачи осуществляется в двух направлениях: обеспечение безопасности информационных процессов и ограничение доступа личности к информации, представляющей собой угрозу ее жизнедеятельности. Более подробно рассмотрим второе направление.

Наибольшее влияние информационно-коммуникативные процессы оказывают на духовную сферу социума, вызывая часто отрицательные последствия и деструктивные изменения в форме психоэмоциональной и социальной напряженности, ложных ориентаций и ценностей и т. п. [1]. Создаваемая обществом современная информационная среда оказывает значительное воздействие и на психологические процессы, и на составляющие в ключевых областях общественной жизни.

Ключевые процессуальные составляющие создаваемой информационной среды представляют собой информационно-коммуникативные процессы, которые оказывают активное воздействие на эмоциональные

части индивидуального, группового и массового сознания. Одной из характерных особенностей процессов, протекающих в информационной среде, является их динамизм.

Вопросы обеспечения информационной безопасности деятельности государственных структур и объектов, учреждений и общественных организаций без учета нужд, и потребностей личности уже продолжительное время являются актуальными, причем и в теоретическом, и в прикладном отношении. Тем не менее, продолжающиеся процессы, связанные с информатизацией общества и информационными войнами, выдвигают на передний план интересы самого человека в информационной сфере и ставят перед наукой и практикой задачи по исследованию и решению практически новой компоненты данной проблемы – информационно-психологической безопасности личности [2-3].

В современных условиях информатизации общества большая часть ученых и практиков обращают внимание на данную проблему и отмечают необходимость ее разработки (В.Е. Лепский, Г.В. Грачев, М.Л. Князева, Т.И. Колесникова, А.К. Грязнов, Е.Л. Доценко, А.А. Журин, и др.).

Узловые источники угроз информационно-психологической безопасности (ИПБ) по отношению к личности рассматриваются, в основном, как внешние и внутренние. К внешним угрозам следует отнести соответственные воздействия разнообразных организаций и людей, средства массовой информации и пр. С этих позиций формирование информационно-психологической безопасности требует создание надлежащей системы противостояния по отношению к внешним угрозам. Такая система должна состоять из нормативно-правовой, организационной и технологической составляющих [4]. При рассмотрении угроз со стороны различных источников информации необходимо обращать внимание на существовании различных типов угроз и их конкретных примерах.

Внутренние источники угроз ИПБ индивида определяются непосредственно индивидуально-личностными характеристиками личности (критичность, внушаемость, импульсивность), а также биологосоциальной природой психики личности, отличительными чертами ее формирования и функционирования [2]. Следовательно, с точки зрения обеспечения информационно-психологической безопасности целесообразно рассматривать личность одновременно и как объект, и как субъект личной безопасности, поскольку отмеченные внутренние факторы и понимание того, что и внешние факторы оказывают деструктивное воздействие опосредовано через внутренний мир человека.

Объективная неосуществимость уберечь личность от всевозможных деструктивных информационно-психологических воздействий сдвигает решение проблемы обеспечения ИБП личности на формирование у человека способности невосприимчивости и устойчивости к подобным психологическим воздействиям, что перемещает данную проблему в психолого-педагогическую плоскость.

Информационно-психологическая безопасность личности В.Е. Лепским определяется как научно-практическое направление, которое сформировано для того «чтобы обеспечить защищенность индивидуумов и сообществ от противозаконных информационных угроз и формирования информационной сферы, соответствующей задачам стимулирования и поддержки рефлексивного способа существования человека (группы) как субъекта жизни (деятельности)» [5-6]. Отмеченные в определении цели (обеспечить защищенность личности и создание требуемой информационной сферы) фиксируют различные подходы к пониманию ИПБ личности и ее обеспечения.

Анализ определений ИПБ личности, приведенных в работах Г.В. Грачева, Г.Л. Смолян, И.К. Мельник, С.Ю. Решетиной и др., указывает на то, что проблема информационно-психологической безопасности личности на основании обоснований замещается проблемой обеспечения защиты индивидуума от деструктивных информационно-психологических угроз. Психологическая защита индивидуума рассматривается как использование разнообразных общепсихологических средств и способов преобразования процессов информационно-психологических коммуникаций личности с информационной средой для исключения или ослабления деструктивных факторов, обладающих способностью причинить ему ущерб» [2, 7].

Следовательно, развитие у индивидуума качеств, способных противодействовать информационным угрозам его психическому состоянию, необходимо направить на выработку у личности необходимой мотивации, знаний и умений, способных обеспечить безопасность человека.

Другой подход, используемый в трактовке информационно-психологической безопасности личности, базируется на умении индивидуума так противодействовать информационным угрозам, чтобы с течением времени не ослабевали бы потенциальные возможности человека в достижении им жизненных целей, и гарантировалось его развитие [2]. Такой подход к обеспечению информационно-психологической безопасности личности основывается на наличие стабильной системы жизненных ценностей и их воплощение в жизнь.

В связи с широким распространением сети Интернет достаточно часто приходится говорить не об ограничении доступа личности к опасной информации, а наоборот, когда контакт пользователя с опасной информацией происходит не как результат его действий, а как результат несанкционированного, вредоносного проникновения такой информации к пользователю. В таком случае данная проблема решается в рамках первого направления, когда распространение опасной информации ограничивается различными техническими или юридическими способами. Если же говорить об ограничении доступа личности к опасной, вредоносной информации, то, кроме принятия определенных технических и законодательных мер, необходимы меры воспитательного воздействия на личность. Особенно актуально такое воздействие в том случае, когда потребителями такой информации являются молодые люди и подрастающее поколение. Именно привитие

соответствующих нравственных убеждений является более эффективным средством ограждения личности от вредоносной информации, причем как от ее потребления, так и от ее создания и распространения. Если кто-то создает компьютерный вирус, заражающий миллионы компьютеров по всему миру, а кто-то посещает сайты с безнравственным содержанием или играет в жестокие компьютерные игры, то причина этого – в наличии пробелов в нравственных убеждениях личности, недостатке ее воспитания.

Основываясь на отмеченных позициях: «знание и понимание себя, в принятии себя и в подлинности личностных проявлений», можно утверждать, что для обеспечения ИПБ личности необходимо развивать ценностно-смысловую сферу человека, его личностные качества, оказывать содействие и помощь в духовно-нравственном становлении. Анализируемые направления на должном уровне согласовываются с современными тенденциями образования, в частности, с вектором его гармонизации, а общие задачи, в своем большинстве, сходны с дидактическими целями общего психологического образования. Поэтому психологическое образование необходимо рассматривать как важную часть образования, способствующую развитию фундамента для формирования информационной и психологической культуры личности.

Современный человек получает из глобальной сети огромные объемы информации. Данное утверждение в значительной степени относится к молодому поколению, члены которого, в своем большинстве, не способны дать правильную нравственную и правовую оценку получаемой информации и своих действий в сети Интернет, поскольку имеют не сформировавшуюся устойчивую систему нравственных качеств и юридических знаний, а фрагментарный набор неких взглядов и убеждений, зачастую противоречивых. Такая система формируется в процессе духовно-нравственного воспитания человека, которое, учитывая увлеченность молодого поколения интернет-технологиями, поэтому логично ее проще реализовывать на пространствах глобальной сети.

При рассмотрении угроз со стороны основных источников информации – телевидения и Интернета – следует акцентировать внимание на существовании различных типов угроз и их конкретных примерах, рассматривать документальные случаи их проявления и последствий. Немаловажным является изучение юридической стороны обеспечения информационной безопасности, тех нормативных актов, которые обеспечивают ее реализацию и предусматривают ответственность за ее нарушение: дети должны понимать, что сеть Интернет – это тоже часть социума и преступления в виртуальном пространстве также недопустимы, как и в пространстве реальном. Процесс такого воспитания целесообразно строить, основываясь на принципах добровольного принятия общепринятых норм поведения, через активное включение молодежи в выполнение общественно полезной и личностно-развивающей деятельности. Именно такое погружение дает возможность найти то общее нравственное начало для современной молодежи и «остального» общества, которому она пытается себя противопоставить, вовлекаясь в антисоциальную деятельность в виртуальном пространстве.

Использование современных информационно-коммуникационных технологий в нравственном воспитании молодого поколения даст ему возможность по-другому посмотреть на окружающий мир, осознать свое место в этом мире и предназначение в жизни, поскольку воспитание имеет своими аспектами не только нравственное, но и патриотическое, гражданское, а также культурологическое просвещение. В условиях компьютерной среды задачи такого воспитания могут быть решены на новом содержательном, продуктивном и техническом уровне.

Ключевые задачи информационного и психологического образования в сфере ИПБ личности целесообразно объединить в несколько блоков:

– создание условий, способствующих формированию у молодых людей и подрастающего поколения самопознания, умений совершенствовать самоконтроль и самоорганизацию;

– содействие в осознании собственной системы ценностей, оказание помощи в выработке личностного подхода для того чтобы справляться с жизненными противоречиями, содействовать выбору правильной жизненной стратегии;

– создание условий, способствующих формированию у молодых людей и подрастающего поколения жизненных взглядов, содействующих выработке позитивного эмоционально-ценностного отношения к себе, к другим людям, к своей безопасности и саморазвитию.

Исследуемые в работе подходы не противоречат друг другу, а сопоставляются как два уровня. В процессе поэтапного формирования индивидуальных качеств личности (знаний, умений, эмоционально-ценностных отношений), содействующих подъему уровня ее защищенности (первый подход) целесообразно перейти к решению вопросов информационно-психологической безопасности индивидуума. Поэтому, в рамках первого подхода следует переходить от предупреждающих к профилактическим мерам.

В рамках второго подхода, заботясь о духовном развитии личности, необходимо переходить от профилактических к созидательным мерам. Рассмотренные оба подхода предполагают постижение психологической действительности и реализуются соответственно в области специального и общего психологического образования.

Использование современных информационно-коммуникационных технологий в нравственном воспитании подрастающего поколения позволит ему по-новому взглянуть на окружающий мир, осознать свое место в этом мире и предназначение в жизни, поскольку воспитание имеет своими аспектами не только нравственное, но и патриотическое, гражданское, а также культурологическое просвещение. В условиях компьютерной среды задачи такого воспитания могут быть решены на новом содержательном, продуктивном и техническом уровне.

Одним из важнейших факторов, обусловливающих успешность учебно-воспитательного процесса, является познавательная активность личности. Ее высокий уровень способствует пониманию и принятию обучающимися целей учебно-воспитательного процесса, побуждает его ответственно относиться к выполнению учебных заданий, делает его субъектом образовательного процесса, а не сторонним наблюдателем. Интерес обучающегося к выполняемой деятельности в значительной степени зависит от его образовательных потребностей, которые, в свою очередь, определяются индивидуальными и общественными условиями его жизни. Познавательный интерес, во многом определяя качество образовательного процесса, тесно взаимосвязан с эмоциональным настроем обучающегося, его творческим отношением к выполняемой деятельности. Выраженный познавательный интерес, положительное эмоциональное отношение к образовательной деятельности могут быть вызваны тем, что деятельность обучающегося связана с его личной и общественной жизнью, теми условиями и тем регионом, в которых он проживает.

Одним из приёмов повышения мотивации обучающихся и стимулирования их познавательного интереса является их включение в исследовательскую деятельность. Для этого при изучении вопросов обеспечения информационной безопасности необходимо ставить перед обучающимися задачи, не только требующие поиска ответа в учебнике или сети Интернет, но и побуждающие их к глубокому изучению поставленной проблемы, ее анализу в контексте своей личной жизненной ситуации, поиску путей решения проблемы и их обоснования, правовой и нравственной оценке ситуации.

Следовательно, можно утверждать, что решение теоретических и практических проблем психологического образования способно внести существенный вклад в повышение уровня информационно-психологической безопасности личности. Обеспечение ИПБ личности является развитие ее ценностно-смысловой сферы и критического мышления, которое всецело и целиком основывается на мировоззрении человека. Кроме того, информационная культура личности может стать одним из краеугольных камней в формировании информационной безопасности личности, так как она является подсистемой личности, которая обеспечивает требуемый характер процессов ее жизнедеятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Костюк А.В., Бобонец С.А., Флегонтов А.В. Информационные системы и технологии. Информационные технологии. Базовый курс. Учебник. Часть 2.– СПб.: Изд. РГПУ им. А.И. Герцена, 2014. – 308 с.
2. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. URL:htpp//bookap.by.ru/psywar/grachev. (дата обращения: 18.09.2017)
3. Бобонец С.А., Костюк А.В. Обеспечение безопасности электронного обучения // Направления и перспективы развития образования в военных институтах внутренних войск МВД России: материалы VII Международной научно-практической конференции: в 2 ч. / Изд-во НВИ войск национальной гвардии. – Новосибирск, 2017. – С.102-104 сЛызь Н.А., Непомнящий А.В. Безопасность как характеристика личности // Известия ТРТУ. Таганрог, 2002. № 5 (28). С. 168–173.
4. Костюк А.В Подходы к информационно-психологической безопасности личности // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 3 / СПОИСУ. – СПб., 2017. С. 52–54.
5. Костюк А.В., Бобонец С.А. Анализ влияния типов организационных структур на информационную безопасность // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 2 / СПОИСУ. – СПб., 2016.– С. 102–104.
6. Костюк А.В., Бобонец С.А. Информационные технологии в науке и образовании. Часть 1. – Учебник. СПб.: Астерион, 2017.– 256 с.
7. Лепский В.Е. Информационно-психологическая безопасность субъекта в изменяющемся обществе /Индивидуальный и групповой субъекты в изменяющемся обществе. М., 1999. С.98–99.

УДК 004.056

УГРОЗЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Костюк Анатолий Владимирович, Николаев Иван Андреевич
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: kostyuk.anatoliy.2015@mail.ru, nikolaev/010101@gmail.com

Аннотация. В статье рассмотрены проблемы информационно-психологической безопасности личности в условиях информатизации общества. Анализируются вновь сформировавшиеся угрозы безопасности личности в обществе на новом этапе его развития. Формулируются направления, реализация которых будет способствовать обеспечению информационно-психологической безопасности личности, предлагаются. способы предотвращения отрицательных последствий деструктивного информационно-психологического воздействия.

Ключевые слова: информационно-психологическая безопасность личности; проблемы безопасности личности; направления обеспечения безопасность личности.

THREATS OF INFORMATION-PSYCHOLOGICAL SECURITY OF PERSONALITY IN INFORMATION SOCIETY

Kostyuk Anatoliy, Nikolaev Ivan
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mails: kostyuk.anatoliy.2015@mail.ru, nikolaev/010101@gmail.com

Abstract. The article discusses the problems of information-psychological security of the individual in the conditions of the informatization of society. Newly formed threats to the security of the individual in society at a new stage of its development are analyzed. Directions are formulated, the implementation of which will contribute to ensuring the informational and psychological security of the individual, are proposed. ways to prevent the negative effects of destructive informational and psychological impact.

Keywords: information-psychological security of the individual; problems of personal security; directions for ensuring the security of the individual

Следует отметить, что характерной чертой развития современного общества становится его информатизация, проявляющаяся в последовательной и систематической разработке и внедрении информационных технологий и информационных средств во все области деятельности человека. В современных условиях информационные ресурсы и информация выполняют важнейшую роль в развитии личности, общества и государства. Отмеченные особенности позволяют утверждать, что информатизация деятельности человека выступает в роли локомотива, ускоряющего развитие человечества и, что это развитие приближает страну к развитому информационному обществу [1-2].

Информационная глобализация, формирование транснациональной инфокоммуникационной инфраструктуры, упрощение доступа пользователей к ее ресурсам, а значит и доступа к информационному пространству извне, порождает угрозы, вызываемые возможным использованием новых инфокоммуникационных технологий, инструментов информационно-психологического воздействия для достижения криминальных целей в информационной сфере, а также в войнах. В процессе ведения как информационных, так и гибридных войн властные структуры проводят широкомасштабные психологические операции, которые направлены против отдельных личностей или социальных групп, выбранных в качестве «мишени» [1-2].

Специальным образом трансформированная информационная среда становится информационным оружием, активно использующимся в политической борьбе. Эти инструменты имеют достаточно широкий диапазон – от создания «фейковых» новостей («малазийский Боинг», «белые каски» в Сирии) и прямого внушения – до использования технологий виртуальной реальности, от простого видеоряда – до нейролингвистического программирования. Человек становится жертвой подобных технологий, что может привести как к разрушению его личности, так и к побуждению выполнять деструктивные действия по отношению к другим членам социума.

Информационная безопасность личности с социально-психологической точки зрения преимущественно ассоциируется с различными информационными воздействиями на психику человека и опасностями, связанными с ними [3].

В первую очередь речь идет о воздействии на индивидуальное сознание человека как члена социума, гражданина, с определенным типом электорального поведения. Политическая реальность современной жизни характеризуется тем, что любые информационно-психологические воздействия, независимо от используемого метода (СМИ, социальные сети, слухи) являются инструментами манипуляции общественным мнением, провокации, спусковым механизмом социальных протестов, что особенно характерно для технологий «цветных революций». Подобные манипуляции человеком, общественным мнением и массовым сознанием наряду с национальными конфликтами, экологическими катастрофами и проблемами демографии уже превратились в мировую проблему и широко используются в информационных войнах. За примером далеко ходить не надо – массированная информационная атака на российское олимпийское движение есть не что иное, как именно информационно-психологическое воздействие на мировое сообщество.

Кроме того, широко применяются информационные воздействия, непосредственно угрожающие физическому или психическому здоровью человека [3]. Сектантство, шаманизм, мистификации различного толка, эзотерика в своих крайних проявлениях, распространение по Интернету мистических учений и практик приводят к разрушению личностных ориентиров человека, а иногда и к разрушению психики человека, вплоть до его физической гибели, пример – группы «смерти» в социальных сетях [4].

Не менее серьезная опасность для здоровья и психики человека является распространение по глобальной сети неприличной и унижающей человеческую нравственность и достоинство информации (порнография), а также недобросовестной рекламы, организация «фишинга» и других мошеннических операций. За счет инфокоммуникационных ресурсов Интернета и социальных сетей, их трансграничности и удобства анонимного доступа, проповедываются преступные идеи и технические материалы криминальных сообществ (рецепты наркотических, отравляющих, взрывчатых веществ), планируется и реализуется подготовка к проведению реальных террористических атак и других криминальных действий.

В качестве негативного фактора информационно-психологической безопасности личности часто выступают и государство (США, Великобритания, Украина и др.), и отдельные недобросовестные лидеры, и политические партии, которые стремятся получить «личную» выгоду, доказать собственную «исключительность», используя властный ресурс для оказания информационно-психологического воздействия на общество для того чтобы скрыть истинные намерения, часто противоречащие интересам населения. Серьезность разрушительного воздействия на психику человека значительно увеличивается в тех случаях, если структуры, обладающие властью, начинают манипулировать сознанием масс или

экспериментировать с ними ради «благих великих целей» и манипулировать их сознанием [4]. В политической истории России, да и в мировой истории вне меньшей степени, можно найти достаточно много примеров.

Новые возможности добавляются к сетевым технологиям при использовании новых технологий мультимедиа и виртуальной реальности, которые используются не только в сфере образования и коммуникации, но могут быть использованы и сфере виртуальных «путешествий». Следует отметить, что подобное «путешествие» может быть небезопасно, так как виртуальной реальности вовлекают человека в новые формы существования и могут влиять на процесс формирования свойств личности [5]. Технологии виртуальной реальности позволяют создавать несуществующие в физическом смысле явления и события, вводят человека в мир, недоступный ему в реальной жизни. За счет «свободного» вовлечения, властные отношения приобретают привлекательность, облекаются в игровую форму, отчасти мистическую, что позволяет, в частности, вывести часть протестных движений в область опросов, петиций и виртуальных флэш-мобов.

Именно в рамках виртуальных систем человек получает легкий доступ к деструктивным для психики эмоциям, не отдавая себе отчета о возможных последствиях. В действительности технологии виртуальной реальности обладают способностью превратить информационное воздействие в индивидуально-ориентированное, направленное на сознание конкретной личности, манипулировать сознанием, погружать человека в состояния, приводящие к фрустрации, мотивировать его к определенным поступкам. Технологии виртуальной реальности, порождая новые формы социального контроля, создают новые возможности для властных структур, подменяя прямой социальный контроль и воздействие опосредованными.

Негативные социально-психологические последствия заключаются в том, что человек может потерять нравственные ориентиры, утратить способность видеть различия между реальным и иллюзорным. Опасна и сама по себе высокая степень псевдореальности, а массовое увлечение новыми технологиями лишь усугубляет эту опасность, особенно в отношении детей и подростков, когда затруднено распознавание истинности происходящего.

Призывы к нравственности потребителей информации, т. е. не посещать сайты сомнительного содержания, не воспринимать информацию сомнительного характера, не использовать программы виртуальной реальности и т. п., являются «гласом вопиющего в пустыне» [6]. Если гипотетически предположить, что совместными усилиями государства и общества удалось запретить или существенно ограничить распространение информации «сомнительного характера» в Интернете, проблема останется в силу многообразия мнений, как экспертного сообщества, так и отдельных пользователей. Фактически, ни государство, ни общество не способны дать полную гарантию человеку в защите его прав и свобод от психологического насилия, а искусственно созданный «высоконравственный человек» может оказаться морально и психически неподготовленным к проявлению по отношению к нему даже незначительной агрессии.

Как показывает практика, даже тоталитарные государства не в состоянии в полной мере ограничить доступ своих граждан к информации «сомнительного характера», да и где найти объективное «мерило» сомнительности информации.

Рассмотренные средства, технологии и специально созданная информация, ненавязчивого манипулирования сознанием, представляет наибольшую опасность для несформировавшихся личностей, поскольку вероятность соприкосновения с любым из источников недоброкачественной информации весьма велика. В результате такого общения можно получить психологическую травму на всю жизнь.

Трансформация и изменение информации или процессов ее функционирования может быть использована некоторыми субъектами для оказания воздействия на психику людей и изменения их поведения, для психологических манипуляций. Специфическим образом организованное изменение информационной среды выступает как своеобразное информационное оружие, которое достаточно активно используется во внутренней и внешней политике многих государств.

В работах по теории информационной безопасности такую безопасность информации относят к группе информационно-психологической безопасности личности, поскольку она определяет условия для обеспечения психического здоровья отдельной личности, а соответственно и населения государства в целом. Вывод напрашивается следующий: долгосрочных и типовых решений по обеспечению безопасности личности в сфере информационно-психологических воздействий не существует.

Одним из последствий, протекающего в настоящее время процесса информатизации, является то, что человек становится информационно «прозрачным». При желании и наличии необходимых средств и технологий информация о конкретной личности, размещенная в аккаунтах или социальных сетях, может превратиться в доступную, и использоваться в различных целях другой личностью или группой лиц.

Проблемы личности и аспекты ее безопасности всегда находились в центре внимания отечественных исследователей, которые предлагают различные меры защиты личности от информационно-психологического воздействия [1,3,4]. Большая часть отечественных исследователей поддерживает правовые формы обеспечения информационно-психологической безопасности личности на законодательном уровне, перенося ответственность на провайдеров или создателей подобной информации, а также рекомендует использование комплексных мер различного характера, которые иногда балансируют на грани запрета свободы слова и свободы личности.

Как показывает опыт, лишь небольшая часть населения обладает способностями предотвратить несанкционированный доступ к своей информации. Основная часть людей такими способностями и возможностями не обладают и являются беззащитными в информационном плане. Следовательно, уровень защищенности информации личностного характера, а также защита от недоброкачественной информации зависит не только от общества, но и от государства.

На ключевой вопрос, как быть и какие шаги предпринимать, чтобы обеспечить безопасность личности в современном обществе, идущим по пути информатизации, целесообразно выделить ряд направлений, реализация которых будет способствовать обеспечению безопасности личности:

– целесообразно прийти к общему пониманию используемых понятий в области обеспечения информационной безопасности личности,

– сформировать общую точку зрения на проблемы деструктивного воздействия информации на психику личности, на индивидуальное и общественное сознание и на политико-идеологическую сферу;

– необходимо разработать и принять международные законодательные акты, которые, не нарушая прав и свобод гражданина, регулировали бы информационные отношения в использовании конфиденциальной информации в компьютерных сетях и системах информационно-коммуникационных технологий, обладающих возможностью реально или потенциально использоваться в террористических и криминальных целях.

Проведенный анализ позволяет сделать промежуточный вывод о том, ключевой проблемой в области обеспечения информационной безопасности личности является явно недостаточная образованность населения в области информационной безопасности.

Формирование психологически устойчивой личности и оперативная реакция государства и общества на негативные информационные процессы в Интернете и СМИ, политика плюрализма и демократии будут способствовать гармоничному развитию личности, общества и государства. Для этого следует учитывать требования времени по обеспечению информационной безопасности в ходе всего воспитательного и образовательного процессов, начиная с дошкольного образования.

Таким образом, знание своих индивидуальных психологических особенностей и закономерностей функционирования психики становится для человека в настоящее время не только обязательным элементом его общей культуры, но и важнейшим условием информационно-психологической безопасности в социуме.

СПИСОК ЛИТЕРАТУРЫ

1. Костюк А.В. Подходы к информационно-психологической безопасности личности // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 3 / СПОИСУ. – СПб., 2017. – С. 52-54.
2. Костюк А.В. Использование информационно-коммуникационных технологий для подготовки офицеров национальной гвардии. // Под общ. ред. С.А. Куценко: сб. науч. ст. международ. науч.-практич. конф. – Новосибирск: НВИ ВВ имени генерала армии И.К. Яковлева МВД России, 2017. – С. 462–466.
3. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности защиты. – М.: изд-во РАГС, 1998. – 125 с.
4. Никитин П.В., Капелькина А.В., Фархшатов И.В. Современные проблемы информационной безопасности личности // Международный студенческий научный вестник. – 2015. – № 6. URL: https://eduherald.ru/ru/article/view?id=14280 (дата обращения: 08.09.2018).
5. Костюк А.В., Бобонец С.А. Анализ влияния типов организационных структур на информационную безопасность. Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 2 / СПОИСУ. – СПб., 2016. – С. 102-104.
6. Костюк А.В., Бобонец С.А. Проблемы информационной безопасности в технологиях дистанционного обучения (статья). Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 2 / СПОИСУ. – СПб., 2016. – С. 100–102.

УДК 004.492.2

БЕЗОПАСНОСТЬ ПРИМЕНЕНИЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Локнов Алексей Игоревич, Примакин Алексей Иванович
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: info_for_aleksey@mail.ru, a.primakin@mail.ru

Аннотация. Рассмотрены возможности и преимущества применения облачных технологий в деятельности подразделений ОВД. Сделан акцент на решении вопросов обеспечения защиты информации по основным критическим областям безопасности облачных технологий: безопасность хранимых данных в облаке, защита данных при передаче, аутентификация, изоляция пользователей, нормативно-правовые вопросы, реакция на происшествия, аудит и организационные меры.

Ключевые слова: облачные технологии; обеспечение безопасности облачных технологий; информационная система обеспечения документооборота МВД России.

SECURITY OF CLOUD TECHNOLOGIES IN THE ACTIVITIES OF INTERNAL AFFAIRS BODIES

Loknov Aleksey, Primakin Alexey
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mails: info_for_aleksey@mail.ru, a.primakin@mail.ru

Abstract. The possibilities and advantages of using cloud technologies in the activities of ATS units are Considered. Focus on the solution of questions of protection of information of key critical security areas of cloud technology: security data stored in the cloud, protecting data in transit, authentication, user isolation, legal issues, incident response, auditing, and organizational measures.

Keywords: cloud technologies, security of cloud technologies; information system of document flow of the Ministry of internal Affairs of Russia.

Большинство специалистов в области информационных технологий считают, что наиболее прогрессивный принцип создания информационных систем – это применение облачных технологий. Преимущества электронного документооборота неоспоримы и состоят в том, что в результате его внедрения все структуры организации смогут функционировать в едином информационном пространстве, обеспечивающем существенное увеличение скорости обработки различных типов документов [1].

Национальный институт стандартов и технологий США предложил называть «облаком» инфраструктуру, которая:

– имеет возможность самообслуживаться по требованию пользователя;

– обладает универсальным доступом посредством сети, охватывая все категории терминальных устройств;

– объединяет ресурсы для возможности обслуживания как можно большего количества пользователей в единственный пул;

– гибкая и эластичная инфраструктура;

– автоматически ведет учет потребления на ходу, подсчитывая использованные ресурсы.

Облачные технологии позволяют хранить файлы в облачных хранилищах, экономя место на локальном жестком диске; нет необходимости использовать специализированное программное обеспечение (например, для проигрывания той же музыки); нет проблем с правами на интеллектуальную собственность (правовые нюансы ложатся на плечи облачного сервиса); обеспечивают доступ к облаку из любого устройства (гаджета), имеющего подключение к сети Интернет.

Концепция облачных технологий включает в себя (как услуги): инфраструктуру, платформу, программное обеспечение, данные и рабочее место.

Основой облачных технологий являются модели предоставления услуг: программное обеспечение, как услуга (SaaS – Software as a Service); инфраструктура, как услуга (IaaS – Infrastructure as a Service) и платформа как услуга (PaaS – Platform as a Service).

SaaS-модель предполагает, что пользователи получают доступ к программному обеспечению по заявкам через сеть Интернет (на основе подписки или аренды). Поставщик услуги обеспечивает хранение пользовательских приложений и данных на серверах «облака», управляет доступом, безопасностью и производительностью приложений.

IaaS-модель предполагает предоставление аренды вычислительных мощностей для создания собственной инфраструктуры в «облаке».

PaaS-модель предполагает предоставление пользователю интегрированной платформы для разработки, тестирования, развертывания и поддержки веб-приложений, расположенной на инфраструктуре «облака» поставщика услуг. Поставщик обеспечивает поддержку работоспособности интегрированной платформы.

Министерство внутренних дел также намерено использовать в своей работе облачные сервисы (удаленные базы данных) и расширять спектр услуг, предоставляемых в электронном виде.

Основные преимущества использования облачных технологий в деятельности подразделений МВД России: минимальные требования к аппаратному обеспечению (обязательное условие – наличие доступа в Интернет); облачные технологии не требуют затрат на приобретение и обслуживание специального программного обеспечения (доступ к приложениям можно получить через окно веб-браузера); поддерживают все операционные системы и клиентские программы, используемые практически в любой сфере деятельности; работа с документами возможна с помощью любого мобильного устройства, поддерживающего работу в Интернете; все инструменты бесплатны. Облачные технологии упрощают доступ к удаленным сервисам, что позволяет не только повысить эффективность функционирования информационных систем, построенных на основе баз данных, но и сократить расходы на приобретение современных продуктов информационных технологий.

Однако существует проблема обеспечения безопасности облачных технологий. В настоящее время основными экспертами в данной области выступают Cloud Security Alliance (CSA) и Trusted Computing Group (TCG). Обе перечисленные организации занимаются стандартизацией и сертификацией облачных технологий.

Компанией Cloud Security Alliance в 2010 году были выпущены рекомендации по безопасности для критических направлений деятельности в облачных вычислениях на 75 листах (Security Guidance for Critical Areas of Focus in Cloud Computing V2.1). Все перечисленные рекомендации можно разделить на шесть основных критических областей безопасности облачных вычислений.

Проведём анализ существующего облака Единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России исходя из безопасности его шести основных составляющих:

1. Безопасность хранимых данных в облаке.

Лучшая мера по защите расположенных в хранилище данных – использование технологий шифрования. Облако всегда должно шифровать хранящуюся на своих серверах информацию клиента для предотвращения случаев неправомерного доступа. Провайдер также должен безвозвратно удалять данные тогда, когда они больше не нужны и не потребуются в будущем. Кроме этого, в облаке на клиентских компьютерах должно обязательно быть установлено антивирусное программное обеспечение.

В рамках подготовки настоящего материала не удалось установить используется ли шифрование пользовательских данных, данных сервисов и баз данных в ИСОД МВД России. Однако стоит отметить, что для работы облака используется ОС Linux, поэтому распределения прав доступа пользователей и шифрования файлов на жестком диске может быть легко реализовано, т.к. поддерживается на уровне операционной системы. Для защиты клиентских компьютеров используется антивирус Касперского с обновлением вирусных баз через внутреннюю сеть МВД России.

2. Защита данных при передаче.

Передаваемые данные всегда должны быть зашифрованы и доступны пользователю только после аутентификации. Такой подход гарантирует, что эти данные не сможет изменить или прочитать ни одно лицо, даже если оно получит к ним доступ посредством ненадежных узлов в сети. Кроме того, крайне желательно, чтобы канал связи между абонентами имел криптографическую защиту для защиты информации от перехвата.

В облаке ИСОД МВД России при доступе на любой сервис используется защищенный протокол HTTPS с шифрованием SSL. Кроме того, для защиты сетевых соединений, как между устройством и сервисом, так и между устройствами используется защищенная сеть VipNet.

ViPNet Client (Клиент) – это программный комплекс, выполняющий на рабочем месте пользователя или сервере с прикладным программным обеспечением функции VPN-клиента, персонального экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования.

Клиент состоит из набора взаимосвязанных программных модулей:

ViPNet (Монитор) – совместно с низкоуровневым драйвером шифрования и фильтрации трафика отвечает за реализацию функций:

1. Персонального сетевого экрана – надежно защищает рабочую станцию/сервер от возможных сетевых атак, как из глобальной (Интернет), так и из локальной сети. При этом осуществляется фильтрация защищенного и открытого трафиков по множеству параметров («белый» и «черный» списки IP-адресов, порты, протоколы); реализуется режим «stealth» (режим инициативных соединений), позволяющий сделать невидимым компьютер защищенной сети из открытой сети; обеспечивается обнаружение и блокировка типичных сетевых атак (элементы IDS).

2. Шифратора IP-трафика – обеспечивает защиту (конфиденциальность, подлинность и целостность) любого вида трафика (приложений, систем управления и служебного трафика ОС), передаваемого между любыми объектами защищенной сети, будь то рабочие станции, файловые серверы или серверы приложений. Высокая производительность шифрующего драйвера, поддерживающего современные многоядерные процессоры, позволяет в реальном времени защищать трафик служб голосовой и видеосвязи в сетях TCP/IP и обеспечивать одновременную работу множества пользовательских сессий.

ViPNet (Контроль приложений) – программа, которая позволяет контролировать сетевую активность приложений и компонент операционной системы. При этом можно формировать «черный» и «белый» списки приложений, которым запрещено или разрешено работать в сети, а также задавать реакцию на сетевую активность неизвестных приложений. В большинстве случаев это позволяет предотвратить несанкционированную сетевую активность вредоносного ПО, например, программ- «троянов».

3. Аутентификация.

Наиболее распространенным способом аутентификации является защита паролем. Однако провайдеры, стремящиеся предложить своим клиентам более высокую надежность, прибегают к помощи более мощных средств, таких как сертификаты и токены. Наряду с использованием более надежных к взлому средств аутентификации провайдеры должны иметь возможность работы с такими стандартами как LDAP и SAML. Это необходимо для обеспечения взаимодействия провайдера с системой идентификации пользователей клиента при авторизации и определении выдаваемых пользователю полномочий. Благодаря этому провайдер всегда будет располагать актуальной информацией об авторизованных пользователях [2].

В ИСОД МВД России для идентификации и аутентификации используется более надёжный механизм SAML (англ. Security Assertion Markup Language – язык разметки декларации безопасности) – язык разметки, основанный на языке XML. Открытый стандарт обмена данными аутентификации и авторизации между участниками, в частности, между поставщиком учётных записей (англ. Identity Provider) и поставщиком сервиса (англ. Service Provider)).

Механизмы SAML в облаке ИСОД реализованы в сервисе управления доступом к информационным системам и ресурсам ИСОД МВД России (СУДИС) предназначен для централизованного управления доступом субъектов доступа (пользователей либо сервисов ИСОД МВД России) к объектам доступа (сервисам ИСОД МВД России).

В данном сервисе проводится идентификация и аутентификация пользователей, после чего СУДИС передаёт сервису из модели SaaS информацию о разрешении доступа или отказе доступа для конкретного пользователя.

Таким образом, данный сервис реализует следующие функции: идентификация и аутентификация пользователей сервиса ИСОД; управление учетными записями пользователей сервиса ИСОД (создание, активация, блокирование и удаление); разделение полномочий пользователей.

Взаимодействие между браузером пользователя, сервисом ИСОД и Сервисом управления доступом происходит в следующем порядке:

– браузер пользователя формирует и отправляет запрос на получение доступа к защищенному ресурсу сервиса ИСОД;

– Сервис ИСОД проверяет наличие в запросе токена доступа, и в случае его отсутствия перенаправляет браузер пользователя в Сервис управления доступом, передавая подписанный запрос на аутентификацию;

– браузер отсылает полученный запрос в Сервис управления доступом;

– Сервис управления доступом отображает пользователю страницу с формами ввода логина и пароля (либо электронной подписи и PIN-кода);

– браузер пользователя передает удостоверяющие данные, введенные пользователем, Сервису управления доступом;

– Сервис управления доступом проверяет удостоверяющие данные пользователя;

– в случае достоверности удостоверяющих данных пользователя Сервис управления доступом перенаправляет пользователя в сервис ИСОД, передавая токен доступа, идентификатор пользователя, атрибуты пользователя и полномочия доступа;

– Браузер пользователя формирует и отправляет запрос на получение доступа к защищенному ресурсу сервиса ИСОД, передавая токен доступа.

4. Изоляция пользователей.

Лучший вариант: когда каждый из клиентов использует индивидуальную виртуальную машину (VirtualMachine – VM) и виртуальную сеть. Разделение между VM и, следовательно, между пользователями, обеспечивает гипервизор.

Некоторые провайдеры помещают данные всех клиентов в единую программную среду и за счет изменений в ее коде пытаются изолировать данные заказчиков друг от друга. Такой подход опрометчив и ненадежен. Во-первых, злоумышленник может найти брешь в нестандартном коде, который позволит ему получить доступ к данным, которые он не должен видеть. Во-вторых, ошибка в коде может привести к тому, что один клиент случайно «увидит» данные другого. За последнее время встречались и те, и другие случаи. Поэтому для разграничения пользовательских данных применение разных виртуальных машин и виртуальных сетей является более разумным шагом.

В качестве основы облака – сервера виртуальных машин или гипервизора в ИСОД используется OpenStack открытое программное обеспечение для разработки инфраструктуры облака на основе ОС Linux. Данный продукт эффективно изолирует виртуальные машины. В работе данной системы периодически обнаруживаются уязвимости, однако разработчики оперативно уведомляют пользователей системы о возникших угрозах и методах по их устранению. В настоящее время на официальном сайте опубликовано постоянно пополняющееся руководство по безопасности – «OpenStack Security Guide».

5. Нормативно-правовые вопросы.

В зависимости от юрисдикции, законы, правила и какие-то особые положения могут различаться. Например, они могут запрещать экспорт данных, требовать использования строго определенных мер защиты, наличия совместимости с определенными стандартами и наличия возможности аудита. В конечном счете, они могут требовать, чтобы в случае необходимости доступ к информации смогли иметь государственные ведомства и судебные инстанции. Небрежное отношение провайдера к этим моментам может привести его клиентов к существенным расходам, обусловленными правовыми последствиями.

Провайдер обязан следовать жестким правилам и придерживаться единой стратегии в правовой и регулятивной сферах. Это касается безопасности пользовательских данных, их экспорта, соответствия стандартам, аудита, сохранности и удаления данных, а также раскрытия информации (последнее особенно актуально, когда на одном физическом сервере может храниться информация нескольких клиентов).

В ИСОД МВД России на данный момент недостаточное правовое обеспечение, однако, существует масса руководящих документов и регламентов, которые могут послужить основой для разработки нормативно-правовых актов [3].

6. Реакция на происшествия, аудит и организационные меры.

Обязательно должны существовать должностные лица, которые занимаются выявлением инцидентов и минимизацией их последствий, информируя пользователей о текущей ситуации. Необходимым требованием к этим лицам является наличие соответствующего специального образования. В рамках МВД России ведётся подготовка специалистов в области информационной безопасности для правоохранительных органов [4-6]. Кроме того, требуются специальные инструменты, направленные на выявление и документирование событий безопасности. В ИСОД МВД России для решения данной задачи применяется программное обеспечение VipNet IDS.

ViPNet IDS – это программно-аппаратный комплекс, выполненный в виде отдельно стоящего сетевого устройства, предназначенный для обнаружения вторжений в информационные системы на основе динамического анализа сетевого трафика стека протоколов TCP/IP для протоколов всех уровней модели взаимодействия открытых систем, начиная с сетевого и заканчивая прикладным уровнем. ViPNet IDS может

использоваться в органах государственной власти Российской Федерации в автоматизированных информационных системах, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну.

Также в качестве системы анализа и контроля защищенности применяется система Positive Technologies Max Patrol разработанная на основе продукта X-Spider.

MaxPatrol позволяет получать объективную оценку состояния защищенности как всей информационной системы, так и отдельных подразделений, узлов и приложений. Механизмы тестирования на проникновение (Pentest), системных проверок (Audit) и контроля соответствия стандартам (Compliance) в сочетании с поддержкой анализа различных операционных систем, СУБД и Web-приложений позволяют MaxPatrol обеспечивать непрерывный технический аудит безопасности на всех уровнях информационной системы. Данный продукт позволяет проводить аудит соответствия рекомендациям российских производителей и государственных стандартов.

Для построения надежной системы безопасности облачного сервиса необходимо соблюдать следующие правила: использовать криптографические средства обеспечения сохранности данных; процесс обмена информацией клиент-сервер должен быть безопасным, т.е. необходимо использовать защищенные протоколы передачи данных, как для доступа к серверу, так и при хранении информации и доступа к информационным ресурсам.

Таким образом, в интересах обеспечения информационной безопасности облачных технологий необходимо осваивать новые методы и средства защиты информации, учитывать инциденты, разрабатывать новые стандарты информационной безопасности, решать вопросы юридического характера. Кроме того, должна быть разработана и внедрена эффективная система мониторинга безопасности облачных технологий применительно к правоохранительной сфере деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Кулемин М. Будущее облачных технологий: европейский взгляд. – М. Бюро Соломатина, 2010.
2. Григорьев В.Р. Проблемы выявления уязвимостей в модели облачных вычислений. Журнал спецтехника и связь, № 4, 2012. – С. 42-46.
3. Кадулин В.Е., Куватов В.И. Обеспечение информационной безопасности облачных технологий в правоохранительной сфере. Труды конференции. Региональная информатика (РИ-2014). XIV Санкт-Петербургская международная конференция. СПб, 2014. – С. 177-179.
4. Примакин А.И., Яковлева Н.А., Локнов А.И. Совершенствование профессиональной подготовки кадров по специальности 10.05.05 – «Безопасность информационных технологий в правоохранительной сфере» для органов внутренних дел. Вестник Рязанского филиала Московского университета МВД России. 2015. № 9. С. 67-74.
5. Воронич В.В., Локнов А.И., Поспелов В.В., Примакин А.И. О совершенствовании некоторых направлений деятельности подразделений Санкт-Петербургского университета МВД России с целью повышения эффективности обучения курсантов по техническим специальностям: 09.03.02 - «Информационные системы и технологии» и 10.05.05 - «Безопасность информационных технологий в правоохранительной сфере». Вестник Санкт-Петербургского университета МВД России. 2015. № 2 (66). С. 162-169.
6. Воронич В.В., Грачев М.И., Локнов А.И., Примакин А.И. Подготовка и переподготовка кадров в области информационной безопасности для правоохранительных органов. Региональная информатика и информационная безопасность Сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 80-84.

УДК 004.056

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ МВД РОССИИ

Саратов Дмитрий Николаевич, Редковников Владислав Александрович
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: saratovdn@mail.ru, iamvladr@gmail.com

Аннотация. В статье предложено решение задачи автоматизации управления информационными рисками в типовых информационно-вычислительных сетях подразделений МВД России. Рассматриваются основные информационные системы и технологии МВД России, понятия «информационный риск» и «управление рисками», основные группы информационных рисков, этапы и стратегии управления информационными рисками, методы их оценки. Предложена математическая модель оценки информационных рисков в информационно-вычислительных сетях МВД России, а также программная реализация данной модели.

Ключевые слова: информационные технологии; автоматизация; информационные риски; оценка информационных рисков; управление рисками.

AUTOMATION OF INFORMATION RISKS MANAGEMENT IN INFORMATION NETWORKS OF MIA OF RUSSIA

Saratov Dmitriy, Redkovnikov Vladislav
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mails: saratovdn@mail.ru, iamvladr@gmail.com

Abstract. In article the solution of the problem of automation of information risk management in standard information networks of MIA of Russia is suggested. Information systems and technologies of MIA of Russia, term “information risk” and “risk management”, groups of information risks, stages and strategies of information risks

management, methods of information risks assessment are considered. Mathematical model of information risks assessment in information networks of MIA of Russia and software implementation of this model are suggested.

Keywords: information technologies; automation; information risks; information risks assessment; risk management.

Введение.

Информационная защищенность в настоящее время является одним из важнейших аспектов общей безопасности на персональном, корпоративном, отраслевом и национальном уровне. Безусловно, этот вопрос в первую очередь затрагивает правоохранительные органы Российской Федерации в лице Министерства внутренних дел. Данное обстоятельство связано с тем, что в современном мире постоянный рост количества используемой информации превратил ее в первостепенный по важности ресурс, который решающим образом влияет на все сферы общественной жизни, отражая тем самым возрастающую информационную зависимость общества. В связи с чем, в упомянутой структуре активно внедряются информационные системы и технологии.

Доказательством активного внедрения в деятельность подразделений МВД России информационных технологий могут служить следующие факты:

– введена в строй и активно используется Единая информационно-телекоммуникационная система органов внутренних дел России, основой которой выступают региональные интегрированные мультисервисные телекоммуникационные системы;

– активно применяются сервисы Единой системы информационно-аналитического обеспечения деятельности МВД России, такие как:

1) сервис электронного документооборота,
2) сервис электронной почты,
3) ведомственный информационно-справочный портал,
4) система видеоконференцсвязи,
5) прикладные сервисы обеспечения оперативно-служебной деятельности полиции;
6) широкое распространение получили интегрированные банки данных общего пользования федерального и регионального уровней, используемые подразделениями МВД России. Суммарное количество объектов учета в перечисленных банках по состоянию на 1 января 2013 года составило чуть более 3,3 миллиардов записей [1].

– для выполнения повседневных обязанностей сотрудниками полиции ежедневно применяются различные технические средства аудио-, фото- и видеофиксации, мобильные аппаратно-программные комплексы (переносные компьютеры, планшеты и т. п.), а также автоматизированные рабочие места, имеющие связь с ведомственными сетями и доступ к ресурсам открытой сети «Интернет».

Важно отметить, что все перечисленные информационные технологии подвержены информационным рискам. Данное обстоятельство связано с тем, что ни одна из существующих на настоящий момент времени информационных технологий не является на сто процентов защищенной и неуязвимой. Любая из них имеет свои индивидуальные уязвимости, которые могут быть использованы в преступных целях, а нарушение работы информационных технологий в самый критический момент может привести не только к высокому материальному ущербу, но и к потере большого количества человеческих жизней.

В связи с этим вопрос оценки и управления информационными рисками является наиболее приоритетным направлением обеспечения информационной безопасности в структурах МВД России.

Понятие «информационный риск», безусловно, связано с наиболее важными свойствами самой информации – конфиденциальностью, целостностью и доступностью.

В.И. Завгородний в своем учебном пособии определяет информационный риск как возможное событие, в результате которого несанкционированно удаляется, искажается информация, нарушается ее конфиденциальность или доступность [2].

Таким образом, становится ясно, что информационный риск представляет собой определенное вероятностное событие, которое негативным образом может повлиять на важную для организации информацию (нарушить конфиденциальность, целостность или доступность информации), что в конечном итоге может привести к нежелательным последствиям.

Необходимо отметить, что информационные риски можно разделить на три основные группы [3]:

– риски, вызванные утратой и/или утечкой информации и использованием ее злоумышленниками или собственными сотрудниками в корыстных целях;

– риски технических сбоев работы аппаратуры и программного обеспечения;

– риски, вызванные непредсказуемыми обстоятельствами (стихийные бедствия).

Согласно стандарту ГОСТ Р 53144-2008 [4], управление рисками представляют собой координированные действия по направлению и контролю над деятельностью организации в связи с рисками.

В классическом управлении рисками информационной безопасности принято выделять пять этапов:

1. Выявление риска и оценка вероятности его реализации и масштаба последствий, определение максимально возможного убытка.
2. Выбор методов и инструментов управления выявленным риском.
3. Разработка риск-стратегии с целью снижения вероятности реализации риска и минимизации возможных негативных последствий.

4. Реализация риск-стратегии.
5. Оценка достигнутых результатов и корректировка риск-стратегии.

Анализ и оценка информационных рисков проводятся на первом этапе, а разработка системы управления рисками – на втором.

Существуют два основных подхода к оцениванию информационных рисков:

– качественная оценка рисков,
– количественная оценка рисков.

В общем случае процесс оценки риска сводится к определению его уровня (качественной либо количественной величины) и сравнении этого уровня с максимально допустимым (приемлемым) уровнем, а также с уровнем других рисков.

В случае проведения качественной оценки рисков применяют качественные шкалы, по которым сначала определяется вероятность проявления той или иной угрозы и уровень ущерба, а затем – сама величина риска.

Зачастую качественные шкалы имеют всего пять градаций (пять уровней):

– очень низкий,
– низкий,
– средний,
– высокий,
– очень высокий.

В таком случае матрица для определения величины риска будет выглядеть, как показано в таблице 1.

Таблица 2

Матрица оценки информационного риска с пятиуровневыми шкалами

Уровень ущерба	Вероятность проявления угрозы				
	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Очень низкий	1	2	3	4	5
Низкий	2	3	4	5	6
Средний	3	4	5	6	7
Высокий	4	5	6	7	8
Очень высокий	5	6	7	8	9

В данном случае минимальному уровню риска соответствует показатель «1», который находится на пересечении очень низкой вероятности проявления угрозы и очень низкого уровня ущерба, а максимальному уровню риска соответствует показатель «9», находящийся на пересечении очень высокой вероятности проявления угрозы и очень высокого уровня ущерба. Для удобства оценку риска можно проводить по интервалу показателей матрицы оценки рисков, например, 1-3 – низкий риск, 4-6 – средний риск и 7-9 – высокий риск.

В случае применения количественной оценки рисков используются количественные оценки показателей и математический аппарат. Значения показателей чаще всего получают путем проведения экспертных оценок, прогнозирования или на основе статистических данных, накопленных на подобных предприятиях и организациях.

Наиболее часто используемыми показателями, применяемыми при количественной оценке информационных рисков, выступают следующие:

– вероятность возникновения негативного события,
– вероятность успешной реализации угрозы,
– коэффициент ценности актива,
– степень уязвимости актива,
– ожидаемое количество попыток реализации угрозы,
– размер предполагаемого ущерба.

Наибольшее распространение получила оценка, проводимая либо по двум, либо по трем показателям – двухфакторная и трехфакторная оценка соответственно.

В простейшем случае производится двухфакторная оценка. Пример проведения двухфакторной оценки информационного риска с учетом вероятности возникновения негативного события и размера предполагаемого ущерба представлен ниже – формула (1).

$$R = P_{события} \times S_{ущерба}, \quad (1)$$

где R – уровень риска,

$P_{события}$ – вероятность возникновения негативного события,

$S_{ущерба}$ – размер предполагаемого ущерба.

Параметр R принимает значения неотрицательных вещественных чисел ([0;+∞)), параметр $P_{события}$ принимает значения от 0 до 1 ([0;1]), а параметр $S_{ущерба}$, как правило, выражается в денежных единицах.

Формула (1) показывает, что, чем выше вероятность возникновения негативного события и чем выше размер предполагаемого ущерба, тем выше становится риск.

Третий этап управления рисками информационной безопасности представляет особый интерес. После проведения качественной или количественной оценки информационных рисков необходимо принять решение о том, каким образом воздействовать на риск для снижения его уровня и уменьшения размера возможного ущерба. В данном случае принимается решение прибегнуть к той или иной стратегии управления информационными рисками. Основными стратегиями управления рисками являются:

- принятие риска,
- избежание риска (уклонение от риска),
- уменьшение риска,
- предотвращение риска и снижение возможного ущерба от него,
- передача риска.

Перспективным направлением в области оценки и управления информационными рисками может выступать автоматизация управления информационными рисками в информационно-вычислительных сетях МВД. Автоматизация данного процесса позволит наиболее эффективно проводить анализ состояния информационных рисков и своевременно снизить их возможное негативное влияние.

Наибольший интерес с точки зрения информационных рисков представляют рабочие места сотрудников и информационно-вычислительная сеть подразделения в целом. Данное обстоятельство обусловлено тем, что один или несколько компьютеров сотрудников, как правило, имеют доступ к сервису электронного документооборота, сервису электронной почты, к интегрированным банкам данных федерального и регионального уровней, а также на данных компьютерах хранится, обрабатывается и передается оперативно-служебная информация, что, безусловно, вызывает интерес у криминальных элементов и средств массовой информации, стремящихся использовать данную информацию в своих целях. В связи с этим компьютеры и сеть подразделения наиболее подвержены информационным рискам.

В качестве математической модели оценки информационных рисков в типовых информационно-вычислительных сетях подразделений МВД России предлагается формула (2).

$$R = P_{НСД} \times \left(K_{ПОМ} + K_{СП} + K_{ИТЗ} + \frac{K_{АО} + K_{ПО} + K_{КС}}{3} \right) \times S_У , \qquad (2)$$

где R – уровень информационного риска,

$P_{НСД}$ – вероятность реализации несанкционированного доступа к информации подразделения,

$K_{ПОМ}$ – коэффициент степени недостаточности правовых и организационных мер,

$K_{СП}$ – коэффициент степени уязвимости сотрудников подразделения,

$K_{ИТЗ}$ – коэффициент степени уязвимости инженерно-технической защищенности подразделения,

$K_{АО}$ – коэффициент степени уязвимости аппаратного обеспечения,

$K_{ПО}$ – коэффициент степени уязвимости программного обеспечения,

$K_{КС}$ – коэффициент степени уязвимости каналов связи и каналов передачи данных,

$S_У$ – предполагаемый ущерб от реализации угрозы.

Автоматизацию оценки информационных рисков целесообразно проводить путем разработки компьютерной программы. Программа должна обладать дружественным интерфейсом, быть простой в использовании и прозрачной для пользователя.

Поведенческая модель программы автоматизированной оценки и управления рисками представлена на рис. 1.

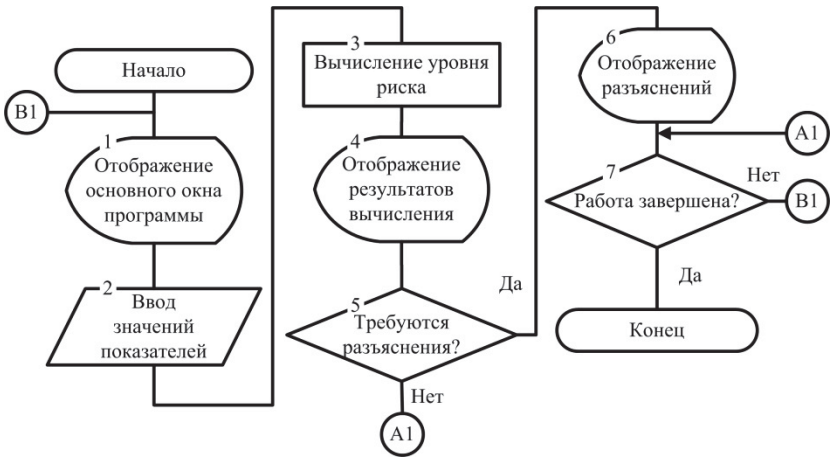


Рис. 1. Поведенческая модель программы

Поведенческая модель программы представляет собой схему алгоритма работы программы. Схема состоит из семи основных блоков, а также блоков начала и окончания работы программы.

Разработку прототипа программной оболочки системы автоматизированной оценки и управления рисками целесообразно вести на языке C++, в среде Borland «C++ Builder» 6 Enterprise Suite. Общий вид основного окна разработанной программы представлен на рис. 2.

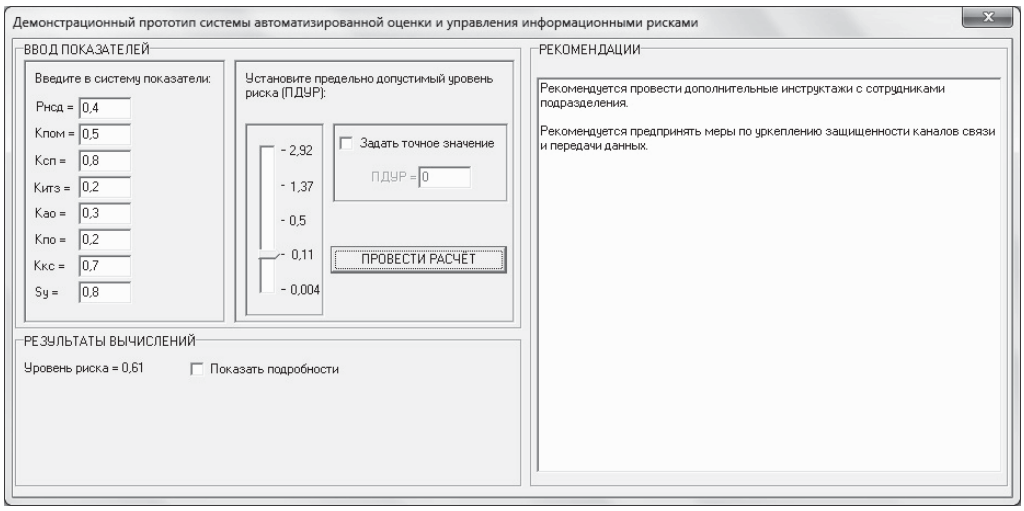


Рис. 2. Общий вид основного окна программы

На основном окне программы располагаются три панели:

– панель «Ввод показателей»,
– панель «Результаты вычислений»,
– панель «Рекомендации».

Панель «Ввод показателей» предназначена для ввода в систему значений показателей в соответствии с математической моделью оценки информационных рисков (формула (2)). Панель «Результаты вычислений» предназначена для вывода результатов проведенных программой расчетов. Панель «Рекомендации» позволяет пользователю ознакомиться с предложенными программой рекомендациями по снижению уровня информационного риска.

Заключение.

Предложенное решение проблемы автоматизации управления информационными рисками в типовой информационно-вычислительной сети подразделения МВД России может повысить эффективность выполнения сотрудниками МВД России задач по оценке и управлению информационными рисками.

СПИСОК ЛИТЕРАТУРЫ

1. Интегрированные банки данных МВД России [Электронный ресурс] : оф. сайт разработ. програм. сист. «Интегрир. банки дан. МВД России» / ЗАО «Инфосеть-С». – Электрон. текстовые дан. – [Москва?], 2014-2018. – Режим доступа: https://www.infonet-c.ru/examples/integrirovannye-banki-dannyx-mvd/ (дата обращения: 24.07.2018). – Загл. с экрана.
2. Завгородний, В.И. Учебное пособие по дисциплине «Информационная безопасность» [Текст] : направление подготовки бакалавра 230700.62 «Прикладная информатика» / В.И. Завгородний ; Финансовый университет при Правительстве Российской Федерации. – М. : Изд-во Финансового ун-та, 2012. – 241 с. : ил., табл.
3. Глухов, Н.И. Оценка информационных рисков предприятия [Текст] : учебное пособие / Н.И. Глухов ; Иркутский государственный университет путей сообщения. – Иркутск : ИрГУПС, 2013. – 148 с. : ил., табл. – 75 экз.
4. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения [Электронный ресурс] : сайт юр. фирмы «Интернет и Право» / А.Г. Серго ; разр. сайта ArtStyle Group. – Электрон. текстовые дан. – М. : Стандартинформ, 2012. – Режим доступа: http://internet-law.ru/gosts/gost/51596/ (дата обращения 24.07.2018). – Загл. с экрана.

УДК 004.056

РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ ОРГАНИЗАЦИОННЫХ МЕРОПРИЯТИЙ И СОВЕРШЕНСТВОВАНИЮ ЗАКОНОДАТЕЛЬСТВА МВД В ОТНОШЕНИИ СОТРУДНИКОВ, ДОПУЩЕННЫХ К СВЕДЕНИЯМ, СОСТАВЛЯЮЩИМ ГОСУДАРСТВЕННУЮ ТАЙНУ

Чудаков Олег Евгеньевич, Попова Наталья Сергеевна, Иванов Даниил Дмитриевич
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: oechuda@yandex.ru, dogslikecats1@gmail.com, danl98@yandex.ru

Аннотация. Проблема защиты государственной тайны встает перед каждым государством, это проблема становиться более актуальной в современном обществе, который характеризуется открытостью общественной жизни и все более развивающимися информационными технологиями, которые также могут быть использованы против независимости Российской Федерации. Организационные методы защиты являются одними из важнейших методов предотвращения раскрытия информации, составляющей государственную тайну, а также её несанкционированный доступ, искажение и уничтожение.

Ключевые слова: безопасность; государственная тайна; режим секретности; организационная защита.

RECOMMENDATIONS FOR THE CONDUCT OF ORGANIZATIONAL ACTIVITIES AND IMPROVING THE LEGISLATION OF THE MOI WITH REGARD TO THE EMPLOYEES APPROPRIATE TO THE STATE SECRET

Chudakov Oleg, Popova Natalia, Ivanov Daniil
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mails: oechuda@yandex.ru, dogslikecats1@gmail.com, danl98@yandex.ru

Abstract. The problem of protecting state secrets rises before each state this problem becomes more urgent in modern society, which is characterized by openness of public life and increasingly developing information technologies that can also be used against the independence of the Russian Federation. Organizational methods of protection are one of the most important methods of preventing the disclosure of information constituting state secrets, as well as its unauthorized access, distortion and destruction.

Keywords: security; state secrets; secrecy regime; organizational protection

Введение.

Безопасность есть одна из характеристик и условий функционирования и развития социальных, экономических, технических, экологических и биологических систем. Вопросы, связанные с обеспечением безопасности государства, всегда остаются актуальными для Российской Федерации. С каждым годом появляются все новые угрозы безопасности государства, что требует постоянного совершенствования существующих методов защиты.

В современном обществе человек, общество и государство выделяются в качестве основных объектов безопасности. Но все развивающаяся информационная сфера жизнедеятельности общества диктует свои правила – информация как основа формирования новых общественных правоотношениях также требует ежедневной и достаточной защиты. В одну из обязанностей государства входит создание взвешенных правовых, организационных и других механизмов защиты различных видов информации, а также учреждение эффективно действующих институтов тайн. Система информационной безопасности Российской Федерации должна обеспечивать надежную охрану конституционных прав и свобод личности, сохранность информации в её первозданном виде, безопасность информационных ресурсов и эффективное функционирование информационных и телекоммуникационных систем.

Институт государственной тайны занимает особое место в системе правоотношений, возникающих при обороте информации и признана многими странами как институт регулирования информационных общественных отношений. Значимость этого института в эпоху формирующегося информационного общества, когда информация приобретает статус одного из основных и ценных ресурсов, невозможно переоценить. Государственная секретность наличествует во всех развитых демократиях мира. Потенциально возможную утечку защищаемой информации за границу государства рассматривают в качестве реальной угрозы своей безопасности. Поскольку за понятием «государственная тайна» стоят не только безопасность государства, но и огромные финансовые средства и активы, труд множества поколений ученых, учебных заведений, научно-исследовательских институтов, экспериментальных баз, инфраструктура и т. д.

Вероятность сохранить все сведения, представляющие ценность, от хищения или уничтожения увеличивается параллельно с уровнем системы защиты информации. Для более глубокого и полного анализа процессов по защите информации, понимания сущности планируемых и проводимых мероприятий, прежде всего, стоит проанализировать одно из важнейших направлений защиты информации - организационную защиту информации.

Введение режима государственной тайны на предприятиях, в учреждения и организациях, обрабатывающих такой вид информации, является одним из необходимых превентивных мер, направленных на сохранение национальных интересов государства в недосягаемости от лиц или организаций, не имеющих доступ к государственной тайны [4].

Нормативное определение государственной тайны сформулировано в ст. 2 Закона РФ «О государственной тайне» [2]. Призму понятия безопасности Российской Федерации, под которой понимается состояние защищенности жизненно важных интересов от внутренних и внешних угроз: государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Закон РФ «О государственной тайне» регламентирует отношения, возникающие в связи с отнесением сведений к государственной тайне, засекречиванием и рассекречиванием сведений, и их защитой в интересах обеспечения безопасности Российской Федерации. Также Закон, в первую очередь, определяет перечень сведений, носящих статус государственной тайны, то есть сведений закрытого характера. На основе данного закона в Министерстве внутренних дел так же действует ряд приказов, регламентирующих отношения в сфере оборота государственной тайны, например, Приказ МВД РФ от 20.08.2010 N 600 «Об утверждении Инструкции о порядке допуска сотрудников, федеральных государственных гражданских служащих и работников органов внутренних дел, военнослужащих и гражданского персонала внутренних войск МВД России к государственной тайне». В сохранении

государственной тайны заинтересован широкий круг физических и юридических лиц, государство, а также общество в целом [7].

Деятельность Министерства внутренних дел тесно связана с получением, использованием и обработкой сведений ограниченного распространения, разглашение которых может повлечь снижение эффективности мер по борьбе с преступностью. Задачи, выполняемые сотрудниками ОВД, предопределяют необходимость обеспечения безопасности информационных ресурсов МВД от утечки важной оперативно-розыскной, разведывательной, политической, экономической, научно-технической и военной информации. Это обосновывает существование института государственной тайны, дающего возможность государству проводить независимую информационную политику, защищать свои национальные интересы. Разглашение или передача сведений, составляющих государственную тайну, по халатности или со злым умыслом, шпионаж в пользу иностранных государств, утрата документов закрытого характера, их опубликование в средствах массовой информации представляют серьезную угрозу государственной безопасности и влечет за собой наложение дисциплинарной, административной или уголовной ответственности. Поэтому государственные власти, в том числе Министерство внутренних дел Российской Федерации, принимают к реализации меры по защите сведений, утечка которых может нанести существенный вред государственным интересам.

В широком смысле слова система мероприятий по защите информации должна создаваться исходя из тех первоначальных условий, которые, в свою очередь, определяются уровнем подготовленности противника, а также целью его разведок, направленных на овладение информацией, подлежащей защите.

Меры организационного характера играют важную роль при решении задач защиты информации, относящейся к государственной тайне, поскольку способны объединить в совокупность все имеющиеся силы, средства, способы и методы защиты информации на основе действующих нормативных актов и правил. Для решения данной задачи необходимы разносторонние знания законодательных основ защиты информации, направлений деятельности подразделений, очередности и порядка принятия управленческих решений в зависимости от выбранного комплекса мероприятий.

Организационные средства защиты, работающие в едином комплексе, позволяют не допустить или существенно затруднить разглашение, утечку и несанкционированный доступ к конфиденциальной информации. Такому результату способствует создание определённой регламентации производственной деятельности исполнителей, связанной с обработкой конфиденциальной информации. Контроль за выполнением организационных мероприятий оп защите проводит первый руководитель, такое правило действует как на государственном, так и на уровне конкретной организации.

Для правильного понимания следует привести два схожих определения понятия организационной защиты [10]:

– организационная защита информации - составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации;

– организационная защита информации - регламентация производственной деятельности и взаимоотношений субъектов (сотрудников) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данной организации.

Первое из приведённых определений в большей степени показывает сущность организационной защиты информации. Второе - раскрывает её структуру на уровне предприятия. Но, в тоже время, оба понятия подчёркивают важность нормативно-правового регулирования, в вопросе защиты информации наряду с комплексным подходом к использованию в этих целях имеющихся сил и средств.

В состав организационной защиты входят следующие направления, которые также реализуются в территориальных органах внутренних дел МВД РФ [8]:

– организация работы с персоналом по недопущению халатного отношения к сохранению государственной тайны;

– организация внутриобъектного и пропускного режимов и охраны с целью предотвращения допуска посторонних граждан к сведениям, составляющим государственную тайну;

– организация работы с носителями сведений, содержащих государственную тайну, на соответствие требованиям, позволяющим определить пригодность носителя к сохранению государственной тайны без изменений;

– организация аналитической работы и контроля с целью предотвращения и прогнозирования возможных каналов утечки;

– комплексное планирование мероприятий по защите информации.

Каждое вышеназванное направление имеет ряд каналов утечки информации ограниченного доступа, которые необходимо максимально сокращать превентивными методами.

Для сотрудников ОВД, работающих с государственной тайной, важнейшим профессиональным качеством является умение хранить сведения, распространение которых может нанести ущерб интересам граждан или государству, и соблюдение режима секретности. Руководство МВД уделяет большое внимание вопросам режима секретности, а проявление высокой бдительности считается юридической обязанностью сотрудников, закрепленной в законодательных и ведомственных нормативных актах. Организационно-методическое руководство деятельностью органов внутренних дел по защите государственной тайны, а также контроль за соблюдением режима секретности, в том числе и в деятельности оперативных подразделений, осуществляются Бюро по защите государственной тайны МВД России, являющимся структурным подразделением Административного департамента МВД России.

В соответствии с Приказом МВД РФ от 20 августа 2010 г. № 600 проверочные мероприятия органов безопасности проводятся в случае наличия сомнений в достоверности предоставленных сотрудниками и кандидатами анкетных данных. Но это дает некоторую вероятность раскрытия государственной тайны в случае необоснованного доверия к кандидату на допуск к государственной тайне. Чтобы такую вероятность исключить необходимо проводить проверочные мероприятия в отношении всех сотрудников с любой формой допуска.

Наибольшие объемы информации закрытого характера проходят через режимно-секретные подразделения, функции которых в органах внутренних дел выполняют управления, отделы, отделения и группы делопроизводства и режима, а там, где их нет, секретариаты, общие отделы и канцелярии. Именно режимно-секретные подразделения планируют, разрабатывают и осуществляют мероприятия по обеспечению режима секретности при проведении секретных работ, принимают меры по выявлению и закрытию возможных каналов утечки сведений, составляющих государственную тайну. Такие подразделения организуют взаимодействие по вопросам защиты государственной тайны. Улучшение взаимодействия с Федеральной службой безопасности Российской Федерации в процессе оперативно-служебной деятельности органов внутренних дел поможет более эффективному выявлению и раскрытию возможных каналов утечки информации ограниченного распространения.

Для организации аналитической работы и контроля в МВД РФ функционирует Центральная экспертная комиссия по режиму секретности [8]. В её состав включаются должностные лица из числа руководителей подразделений центрального аппарата министерства, их структурных подразделений, подразделений, непосредственно подчиненных МВД России. Персональный состав комиссии утверждается министром. Перед комиссией стоит достаточно широкий круг задачи обязанностей. Это контроль за исполнением единых нормативных требований к организационной защите государственной тайны в системе МВД России. Это распространение положительного опыта работы федеральных органов исполнительной власти, научных достижений по обеспечению защиты государственной тайны, перспективных средств защиты информации.

Носители информации, составляющей государственную тайну, также должны в обязательную очередь проходить процедуру оценки соответствия на пригодность к надежной сохранности государственной тайны. А учёт и хранение таких носителей должны исключать искажение, хищение, модификацию и уничтожение информации.

На сегодняшний день, существует некоторое количество проблем в сфере защиты государственной тайны в ОВД. Во-первых, необходимо неоднократно обращать внимание всех работников органов внутренних дел на необходимость правильного обращения с информацией закрытого характера. Во-вторых, это - твердое знание и неуклонное исполнение служебных обязанностей лицами, допущенными к государственной тайне.

Заключение.

За прошедшие 25 лет с момента принятия Закона РФ «О государственной тайне» в Российской Федерации проделана большая работа по созданию механизмов его реализации. Подготовлено и издано более 70 нормативно-правовых актов по вопросам защиты государственной тайны, в том числе около 30 указов и распоряжений Президента и более 40 постановлений и распоряжений Правительства Российской Федерации. Это свидетельствует о том, что законодательство, касающееся функционирования института государственной тайны, не достигло ещё своего совершенства и с каждым вновь принятым нормативно-правовым актом подстраивается в реалии современного общества.

Уровень информационной культуры общества влияет на некоторые проблемы защиты информации, в особенности государственной тайны. Одной из важнейших частей этой культуры является понимание обоснованности и легитимности установления правовых норм в отношении информации ограниченного доступа и в особенности государственной тайны. Эффективное функционирование института государственной тайны – это одно из условий деятельности самого государства, обеспечения его суверенитета, реализации его претензий на достойное место в мировом сообществе [11].

Тенденции увеличения открытости государства перед обществом хотя и диктует необходимость сокращения числа сведений, относимых к государственной тайне, но всё же каждое государство обладает сведениями, имеющими особую ценность, необходимыми для функционирования государства как независимой единицы мирового сообщества.

СПИСОК ЛИТЕРАТУРЫ

1. Конституция Российской Федерации (ред. (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 21.07.2014 N 11-ФКЗ)// [Электронный ресурс] – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/, свободный. – Загл. с экрана
2. Федеральный закон № 5485-1 от 21.07.1993 (ред. 29.07.2018) «О государственной тайне» // [Электронный ресурс] – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/ свободный. – Загл. с экрана
3. Федеральный закон № 380-ФЗ от 28.12.2010 (ред. от 05.10.2015) «О безопасности» // [Электронный ресурс] – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/. – Загл. с экрана
4. Указ Президента РФ № 1203 от 30.11.1995 (ред. 03.09.2018) «Об утверждении перечня сведений, отнесенных к государственной тайне» // [Электронный ресурс] – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_8522/, свободный. – Загл. с экрана
5. Распоряжение Президента Российской Федерации от 16.04.2005 (ред. 22.12.2017) № 151-рп «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне» // [Электронный ресурс] – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71740732/, свободный. – Загл. с экрана
6. Постановление Правительства РФ от 06.02.2010 N 63 (ред. от 29.12.2016) «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» // [Электронный ресурс] – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_97474/ свободный. – Загл. с экрана

7. Приказ МВД России от 20.08.2010 600 «Об утверждении Инструкции о порядке допуска сотрудников, федеральных государственных гражданских служащих и работников органов внутренних дел, военнослужащих и гражданского персонала внутренних войск МВД России к государственной тайне» // [Электронный ресурс] – Режим доступа: http://base.garant.ru/12180121//, свободный. – Загл. с экрана
8. Приказ МВД России от 20.06.2012 N 615 (с изм. от 28.12.2016) «Об утверждении Инструкции по делопроизводству в органах внутренних дел Российской Федерации» // [Электронный ресурс] – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/, свободный. – Загл. с экрана
9. Приказ МВД России от 11 марта 2012г. № 015 «О мерах по обеспечению режима секретности в органах внутренних дел Российской Федерации» // [Электронный ресурс] – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=539374#023787936220625938 /, свободный. – Загл. с экрана
10. Валова С. Надбавка за государственную тайну сотрудникам МВД // Силовые министерства и ведомства: бухгалтерский учет и налогообложение. 2016. N 6. С. 56 - 62
11. Вус М.А., Федоров А.В. Государственная тайна и ее защита в Российской Федерации // Издательство: СПб: Юридический центр Пресс, 2008

УДК 004.056

АСПЕКТЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ ЗАЩИТЫ ЛИЧНОСТИ

Ярмоленко Наталия Владимировна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: nv_yarmolenko@mail.ru

Аннотация. В статье поясняется содержание информационно-психологической защиты личности, раскрываются основные источники угроз информационно-психологической безопасности.

Ключевые слова: безопасность личности; социальные практики безопасного поведения; личность как объект безопасности.

ASPECTS OF INFORMATION-PSYCHOLOGICAL PROTECTION OF THE PERSON

Yarmolenko Natalia
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mail: nv_yarmolenko@mail.ru

Abstract. The article explains the content of information-psychological protection of the individual and reveals the main sources of threats to information-psychological security.

Keywords: personal security; social practice safe behavior; the person as an object of security.

Повсеместное использование различных коммуникационных средств и информационных технологий связывают с разнообразными информационными воздействиями на психику человека, поэтому изучение механизмов действия угроз информационно-психологической безопасности личности является постоянной потребностью не только в повседневной жизни человека и его социальной практики, но и в профессиональной деятельности. Такие угрозы рассматривается как целенаправленные действия конкретных носителей враждебных намерений, воздействуя на объект – личность человека, а так же на его психическое стойкость и профессиональные навыки.

К средствам информационно-психологического воздействия наличность относят, прежде всего, убеждение и внушение (суггестия), формируя определенные жизненные установки и поведение. Кроме того, визуальные методы заставляют личность воспринимать информационно-психологическое воздействие очень быстро, влияя не только на интеллект, но и на эмоционально-чувственную сферу человека. Для программирования определенных действий человека используются гипнотические методы. Более сложное информационно-психологическое воздействие на личность оказывают методы «феноменолигические» методы. На практике используют одновременное применение (комбинирование) нескольких методов или средств воздействия, при этом допускаются не только гуманные, но и антигуманные приемы в сочетании со средствами вооруженной борьбы для достижения максимальной результативности.

Таким образом, манипуляции человеком, общественным мнением и массовым сознанием деструктивного характера могут наряду с межнациональными конфликтами, экологическими бедствиями и демографическими катастрофами превратиться в глобальную проблему для человечества современной эпохи.

Если свойства объекта безопасности ухудшаются посредством насильственного изменения, то угроза выступает в качестве возможности разрешения противоречия во взаимодействии объекта безопасности с другими объектами. Для защиты от внешних угроз разрабатываются специальные меры и локализация их ущерба. Основными характеристиками угроз представляются не только место проявления источника, но и его форма, вероятность предполагаемого ущерба, а также тип объекта безопасности. Для защиты от внешних угроз разрабатываются специальные меры, а также локализация их ущерба.

Под психологической защитой личности подразумевается сложная система личностных механизмов предотвращения или нейтрализации угрожающих факторов, которые наносят ущерб человеку посредством использования различных средств и способов изменения процессов его информационно-психологического взаимодействия с различными социальными субъектами и информационной средой в целом. Благодаря

интенсивному развитию открытых компьютерных сетей и новых информационно-коммуникационных технологий, размещение информационного ресурса на электронных носителях и увеличение концентрации информации в информационных системах различного рода, проблема защиты личных информационных ресурсов становится более актуальной.

Развитие сетевых технологий и технологий мультимедиа дало появлению еще одного вида воздействия на личность индивидуума как виртуальная реальность. Она предлагает новые возможности не только в сфере досуга и культуры, обещая новые несуществующие миры и переживания; интересные идеи «путешествий», но не географического плана. Такие виртуальные путешествия, как правило, небезопасны для личности. Такая технология таит в себе опасность манипулирования личностью и экспериментам над сознанием, апробируя новые методики психотренинга. Конечно, визуальные системы предлагают человеку легкий доступ к событиям и сюжетам, которые могут быть деструктивными для психики. Погружаясь в такие виртуальные реальности, человек не отдает себе отчета, куда это повлияет на состояние его психики.

Угрозы безопасности личности информационно-психологического характера, осуществляя разрушающие воздействия на психологическое состояние личности, препятствуют полноценно развиваться ему и приспосабливаться к сложным социальным условиям, но при этом удовлетворяют его потребности и реализовывая гарантированные Конституцией, нормами федерального законодательства и международного права гражданские права и свободы. Угрозы информационно-психологической безопасности личности воздействуют не только на сознание человека, но и на систему его ценностей, психическое здоровье и свободу воли человека. Потребность в безопасности является необходимым условием нормального существования и развития. Поэтому человек так нуждается в ощущении своей связи с окружающим миром, другими людьми, в принадлежности к определенным социальным группам и общественным структурам.

Рекомендуемые способы обеспечения информационно-психологической безопасности предлагают уход (отказ, отклонение от негативного воздействия), не восприятие негативной информации, блокирование критического восприятия или маскировка проявления своих эмоций. Таким образом, формируется информационная культура сотрудника, что и обеспечивает информационно-психологическую безопасность личности.

Источниками воздействия информационно-психологического характера на личность могут быть:

– государство (в том числе – иностранные государства), органы власти и управления и другие государственные структуры и учреждения;

– общество (различные общественные, экономические, политические и иные организации, в том числе зарубежные);

– различные социальные группы (формальные и неформальные, устойчивые и случайные, большие и малые по месту жительства, работы, учебы, службы, совместному проживанию и, проведения досуга и т.д.);

– отдельные личности (в том числе представители государственных и общественных структур, разнообразных социальных групп и т.п.) [1].

Отечественные исследователи, такие как Г.В. Грачев, Д.А. Ершов, С.К. Рощин, В.А. Соснин, предлагают различные меры защиты личности от информационно-психологического воздействия и поддерживают правовые формы решения проблемы на законодательном уровне, перенося ответственность на провайдеров или потребителей информации. К важным правовым актам противодействия угрозам информационно-психологической безопасности необходимо считать следующие:

1. Защита информации, представляющей угрозу интересам всех субъектов и объектов РФ, от несанкционированного доступа.

2. Мониторинг информации о субъектах и объектах экстремисткой и террористической деятельности.

3. Мониторинг анонимных денежных потоков в сети Интернет.

4. Противодействие пропагандистским устремлениям экстремисткой и террористической идеологии.

5. Рассмотрение технической и правовой возможности привязки пользователя (или технического средства) к информации, выложенной в Интернете [3].

Но процессы информационно-психологического воздействия на человека могут изменяться как им самим, так и в его интересах другими людьми и социальными субъектами различного уровня сложности, системно-структурной и функциональной организации. Иными словами, психологическая защита личности – это использование разнообразных средств и способов изменения процессов информационно-психологического взаимодействия человека с различными социальными субъектами и информационной средой в целом для предотвращения или нейтрализации угрожающих факторов, способных нанести ему ущерб. Модель информационно-психологической защиты, как показывает практика, может включать в себя не только профессионально-психологическую ориентацию и отбор, но и дальнейшую психологическую подготовку специалиста.

Для сотрудника может представлять информационно-психологическую опасность деятельность различных группировок и объединений людей, в частности, некоторых политических партий, общественно-политических движений, националистических и религиозных организаций, финансово-экономических и коммерческих структур, лоббистских и мафиозных групп.

Таким образом, благодаря развитию информационных технологий расширяются методы негативного информационно-психологического воздействия на личности, наблюдается эволюция различных форм терроризма, где огромное значение приобретает информационно-психологическая составляющая. Средства

психологической защиты личности связаны с изменением процессов ее информационно-психологического взаимодействия с информационной средой для предотвращения или нейтрализации угрожающих факторов, способных нанести ущерб человеку. Важнейшим и приоритетным направлением деятельности правоохранительных органов должно стать обеспечение необходимого уровня безопасности обрабатываемой информации, надежная защита сознания и психики личности от негативного информационного воздействия.

СПИСОК ЛИТЕРАТУРЫ

1. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г.В. Грачев. – М.:, 2003.
2. Манойло А.В. Государственная информационная политика в особых условиях. Монография, М. 2003.
3. Примакин А.И. Куватов В.И., Якушев Д.И. Противодействие террористическим и экстремистским организациям в сети Интернет [Текст] // Вестник Санкт-Петербургского университета МВД России. 2015. № 1 (65) – С. 91-95.

УДК 519.2

КЛАСТЕРНЫЙ АНАЛИЗ КАК ИНСТРУМЕНТ ДЛЯ ОБРАБОТКИ ДАННЫХ ПСИХОЛОГИЧЕСКИХ ИССЛЕДОВАНИЙ

Ярмоленко Наталия Владимировна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: nv_yarmolenko@mail.ru

Аннотация. Поясняется использование методов математической статистики для обработки данных психологических исследований. Формулируются задачи кластерного анализа, анализируются свойства кластера и понятие расстояния и мера близости между объектами.

Ключевые слова: кластер; кластерный анализ; выборочная совокупность; матрица.

CLUSTER ANALYSIS AS A TOOL FOR DATA PROCESSING PSYCHOLOGICAL RESEARCH

Yarmolenko Natalia
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mail: nv_yarmolenko@mail.ru

Abstract. The paper explains the use of mathematical statistics methods for processing psychological research data. The problems of cluster analysis are formulated, the cluster properties and the concept of distance and proximity between objects are analyzed.

Keywords: cluster; cluster analysis; sample set; matrix.

Последние достижения в развитии информационных технологий позволяют пользователю с минимальными навыками работы на современных IBM-совместимых персональных компьютерах успешно применять их на практике для различных вычислительных процедур прикладного статистического анализа, в том числе и для психодиагностического обследования. Автоматизация наиболее трудоемких операций обработки и анализа массивов психодиагностических данных выполняется с целью:

– диагностики индивидуальных особенностей (личностных качеств), личностно-профессионального становление, мотивационный профиль и психологического сопровождения личного состава;

– выявления лиц, склонных к срывам социально-психологической адаптации и девиантным формам поведения;

– психологического сопровождения боевого дежурства (боевой службы), караульной и внутренней (дежурной, вахтенной) служб;

– оценки актуального психологического состояния, как отдельных военнослужащих, так и воинских коллективов (подразделений, смен, караулов и т.п.);

– изучения социально-психологических процессов в группах и воинских коллективах (оценка психологической совместимости, профилактика конфликтов, комплектование малых групп для выполнения особо ответственных заданий);

– психодиагностического обеспечения кадровых решений;

– оценки функциональной готовности к выполнению профессиональных обязанностей, оценки влияния факторов деятельности на работоспособность и др.

Последние достижения в развитии информационных технологий позволяют пользователю с минимальными навыками работы на современных IBM-совместимых персональных компьютерах успешно применять их на практике для различных математических процедур прикладного статистического анализа.

Как известно, особенно актуальной проблема трудоемкости становится при многомерном анализе данных. Поэтому эффективная, грамотная, всесторонняя статистическая обработка данных даже небольшого объема практически невозможна без использования вычислительной техники.

Благодаря функциональным возможностям современного компьютера обрабатывать большие объемы информации, информационные технологии сделали доступными для широкого пользователя самые современные

методы статистического анализа. Разработанные статистические пакеты прикладных программ представляют современную форму программного обеспечения для овладения основами статистических методов.

На современном этапе изучение психологических явлений проводят с применением квалифицированно организованного неоднородного выборочного наблюдения с целью получить вероятностные оценки параметров исследуемого объекта или процесса в условиях значительной экономии времени, экономических и финансовых ресурсов. Благодаря уменьшению объема изучаемой совокупности, таким образом, используется объективная возможность углубить программу исследования, т.е. получить более детальную информацию об объекте изучения. Военный психолог стоит перед лицом множества индивидуальных наблюдений, характеризующих их параметров и выявление структуры взаимосвязей между ними. И поэтому применение методов многомерного статистического анализа необходимо для принятия обоснованного решения, оценки надежности и точности выводов [1].

Для разделения неоднородной совокупности наблюдаемых объектов на однородные группы, классифицировать эти группы наблюдения выполняет кластерный анализ, разделяя их таким образом, что в каждой группе они похожи друг на друга больше, чем объекты из других классов. Такие группы называют кластерами. Итак, задача, которая стоит перед кластерным анализом, состоит в разбиении множества объектов на определенное количество кластеров таким образом, чтобы каждый объект выборочной совокупности принадлежал одному кластеру (подмножеству объектов) с определенными свойствами.

Обычной формой представления исходных данных в задачах кластерного анализа служит матрица

$$X = \begin{pmatrix} x_{11} & \dots & x_{1j} & \dots & x_{1k} \\ \dots & \dots & \dots & \dots & \dots \\ x_{i1} & \dots & x_{ij} & \dots & x_{ik} \\ \dots & \dots & \dots & \dots & \dots \\ x_{n1} & \dots & x_{nj} & \dots & x_{nk} \end{pmatrix},$$

каждая строка которой представляет результаты измерений k рассматриваемых признаков у одного из обследованных объектов. В конкретных ситуациях может представлять интерес, как группировка объектов, так и группировка признаков. В тех случаях, когда разница между двумя этими задачами не существенна, например, при описании некоторых алгоритмов, мы будем пользоваться только термином «объект», включая в это понятие и термин «признак» [2].

Оставшиеся объекты принадлежат другим кластерам с иными свойствами. К этим свойствам и относят плотность, дисперсия, размеры, форма и отделимость. Плотность − это свойство, которое позволяет определить кластер как скопление точек в пространстве данных, относительно плотное по сравнению с другими областями пространства, содержащими либо мало точек, либо не содержащими их вовсе. Дисперсия характеризует степень рассеяния точек в пространстве относительно центра кластера, т.е. насколько близко друг к другу расположены точки кластера. Свойство кластера − размеры - тесно связано с дисперсией; если кластер можно идентифицировать, то можно измерить и его «радиус». Это свойство полезно лишь в том случае, если рассматриваемые кластеры являются гиперсферами (т.е. имеют круглую форму) в многомерном пространстве, описываемом признаками. Форма − это расположение точек в пространстве. Если кластеры имеют удлиненную форму, то вместо размера можно вычислить его «связность» - относительную меру расстояния между точками. Отделимость характеризует степень перекрытия кластеров и насколько далеко друг от друга они расположены в пространстве [3].

В кластерном анализе различают понятие расстояния и меру близости между объектами. Меры близости отличаются от расстояний тем, что они тем больше, чем более похожи объекты. Каждый элемент совокупности – это отдельный кластер и между кластерами по какой-то из описанных выше формул найдено расстояние в виде матрицы *D*, симметричной относительно главной диагонали:

$$D = \begin{pmatrix} d_{11} & d_{12} & \dots & d_{1n} \\ d_{21} & d_{22} & \dots & d_{2n} \\ \dots & \dots & \dots & \dots \\ d_{n1} & d_{n2} & \dots & d_{nn} \end{pmatrix}, \quad (1)$$

где $d_{ij} = d(Y_i, Y_j)$.

Из всех расстояний выбираем наименьшее и объединяем соответствующие этому расстоянию элементы в одну группу (кластер). В результате два столбца (и две строки) матрицы преобразуются в один. Пересчитываем на основе одного из принципов расстояния между вновь образованным кластером и остальными элементами. Получаем новую матрицу расстояний D_1, в которой будет на одну строку и один столбец меньше по сравнению с D. Далее в матрице D_1 находим минимальное расстояние и аналогично объединяем соответствующие кластеры и т. д. Процесс может быть закончен на любой стадии в зависимости оттого, какое количество групп требуется в задаче.

Для того чтобы выяснить, входят ли два конкретных элемента в одну группу или нет, необходимо определить некую меру близости между ними. Иначе говоря, необходимо ввести в рассмотрение некую формулу, которая определяет расстояние между двумя различными объектами. В качестве этой формулы достаточно часто используются:

1. Евклидово расстояние:

$$d_{ij} = d(Y_i, Y_j) = \sqrt{\sum_{k=1}^{m} (x_{ki} - x_{kj})^2}. \quad (2)$$

2. Квадрат Евклидова расстояния:

$$d_{ij} = d(Y_i, Y_j) = \sum_{k=1}^{m} (x_{ki} - x_{kj})^2. \quad (3)$$

3. «Взвешенное» евклидово расстояние:

$$d_{ij} = d(Y_i, Y_j) = \sqrt{\sum_{k=1}^{m} w_k (x_{ki} - x_{kj})^2}. \quad (4)$$

4. Хеммингово расстояние:

$$d_{ij} = d(Y_i, Y_j) = \sum_{k=1}^{m} |x_{ki} - x_{kj}|. \quad (5)$$

5. Расстояние Чебышева:

$$d_{ij} = d(Y_i, Y_j) = \max_{1 \le k \le n} |x_{ki} - x_{kj}|. \quad (6)$$

Из всех расстояний выбираем наименьшее и объединяем соответствующие этому расстоянию элементы в одну группу (кластер) [4]. В результате два столбца (и две строки) матрицы преобразуются в один. Пересчитываем на основе одного из принципов расстояния между вновь образованным кластером и остальными элементами. Получаем новую матрицу расстояний D_1, в которой будет на одну строку и один столбец меньше по сравнению с D. Далее в матрице D_1 находим минимальное расстояние и аналогично объединяем соответствующие кластеры и т. д. Процесс может быть закончен на любой стадии в зависимости оттого, какое количество групп требуется в задаче.

В психологических исследованиях объектами для кластеризации могут быть как испытуемые, так и признаки (шкалы психодиагностических методик, показатели социально-демографических характеристик и т.д.), а также корреляции, результаты социометрии и т.д.

Особенности мотивационного профиля личности военнослужащего исследованы математической процедурой кластерного анализа для решения вопроса о группировке испытуемых. Программная реализация алгоритмов кластерного анализа широко представлена в различных инструментах Data Mining, которые позволяют решать задачи достаточно большой размерности. Например, агломеративные методы реализованы в пакете SPSS, дивизимные методы – в пакете Statgraf.

Для разбиения объектов на кластеры использованы иерархические англомеративные методы кластерного анализа. К первому кластеру отнесены испытуемые с высокими значениями, как активности, так и общения, но невысокими показателями состояния устремлений и житейского состояния. Во второй кластер отправили испытуемых с высоким показателем мотивационного профиля устремления как житейского, так и учебного, а также социального статуса. В третьем кластере отнесены испытуемые, обладающими значительными значениями житейского (идеального) состояния, но с невысокими показателями общественной полезности. Четвертый кластер характеризуется высокими показателями житейского (идеального) состояния, однако показатель учебное идеальное имеет низкую величину. В пятый кластер отправили испытуемых с показателями профессионального (реального) состояния высокими, но показатель учебного (идеального) – низкого уровня.

Анализируя полученные итоги исследования, необходимо обратить внимание на тот факт, что в мотивационном профиле испытуемых превалирует аппарат социального поддержания жизненного процесса и потребления, однако, значительно выше идеальная повседневная и идеальная рабочая мотивация. Таким образом, высокий показатель идеальной мотивации говорит о наличии развивающихся мотивов, значительном уровне побуждения и устремления. Наиболее показательные признаки, которые характеризуют исследуемую выборку испытуемых, представлены показателями: поддержание жизнеобеспечения и идеальное положение устремлений. Если вести классификацию мотивационного профиля, то при этом выделяют группу акмеориентированных испытуемых (кластер 1), выбравших образовательную направленность, где наблюдается поступательное прогрессивное личностно-профессиональное развитие, и группу, имеющую затруднения в собственном становлении (кластер 5).

Оценка мотивационного профиля студентов позволяет констатировать, что испытуемые, обладающие выраженной духовной и гражданской направленностью, ориентированы на развитие, творческий подход к решению возникающих задач, удовлетворение личных мотивов в контексте социальных интересов. Их личностно-профессиональное становление предполагает непрерывный процесс саморазвития.

Таким образом, кластерный метод позволяет разделить неоднородную совокупность наблюдаемых объектов психологического исследования на однородные группы, элементы которых характеризуются многими признаками, или близкие по определяющим критериям группы (кластеры), пригодные для дальнейшего исследования. В случае необходимости как-то систематизировать большие объемы информации пригодным для дальнейшей обработки, кластерный анализ оказывается весьма полезным и эффективным.

СПИСОК ЛИТЕРАТУРЫ

1. Айвазян С. А. Многомерный статистический анализ и эконометрика. Труды VIII Международная школы-семинары «Многомерный

статистический анализ и эконометрика», Цахкадзор, Республика Армения [Текст]: труды / Центральный экономико-математический ин-т РАН [и др.]. - Москва: ЦЭМИ РАН, 2012. - 216 с.
2. Айвазян С.А., Мхитарян В.С. Прикладная статистка и основы эконометрики. Учебник. - М: ЮНИТИ, 1998. – 1022 с.
3. Ким Дж.-О., Мьюллер Ч.У. и др. Факторный, дискриминантный и кластерный анализ. Под ред. И.С. Енюкова. – М.: Финансы и статистика, 1989. – 215 с.
4. Мандель И.Д. Кластерный анализ. – М.: Финансы и Статистика, 1988. – 176 с.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ

УДК 336.719

МАТЕМАТИКО-СТАТИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ УВЕЛИЧЕНИЯ ДОЛГА НАСЕЛЕНИЯ ПЕРЕД БАНКАМИ

Большакова Людмила Валентиновна, Смолина Яна Николаевна, Яковлева Наталья Александровна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: blv5505@mail.ru, vasyapetrov95_00@mail.ru, kumirova@mail.ru

Аннотация. В статье рассмотрена проблема увеличения долга населения Российских граждан перед банками, связанная с невыплатой кредита. Приведены данные корреляционного анализа зависимости между величиной долга, суммой ипотечных кредитов, объемом автокредитов и уровнем безработицы на основе статистических данных прошлых лет.

Ключевые слова: долг населения; ипотечное кредитование; автокредиты; уровень безработицы; парный коэффициент корреляции; частный коэффициент корреляции.

MATHEMATICAL-STATISTICAL STUDY OF THE INCREASE OF THE POPULATION DEBT TO BANKS

Bolshakova Lyudmila, Smolina Jana, Yakovleva Natalia
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mails: blv5505@mail.ru, vasyapetrov95_00@mail.ru, kumirova@mail.ru

Abstract. The article considers the problem of increasing the debt of the population of Russian citizens to banks associated with non-payment of the loan. The data of correlation analysis of the relationship between the amount of debt, the amount of mortgage loans, the volume of car loans and the level of unemployment on the basis of statistical data of previous years.

Keywords: debt of the population; mortgage lending; car loans; unemployment rate; pair correlation coefficient; private correlation coefficient.

Введение.

Одной из важных проблем, стоящих перед банковской системой, является возврат кредита, выданного банком населению. Ее решение связано с исследованием возможности уменьшения долга населения перед банками при условии увеличения или, по крайней мере, не уменьшения общей суммы кредитования.

В настоящее время значительно растет общая сумма кредитов и их количество. Так, например, общий размер выданных за год ипотечных кредитов увеличился на 42% до 1,8 трлн руб., а количество – почти на треть и составило 959 237 шт. По подсчетам аналитической компании «Русипотека», 53% выдач ипотечных жилищных кредитов в прошлом году обеспечил Сбербанк. Выдачи автокредитов за весь 2017 год, по данным Объединенного кредитного бюро (ОКБ), увеличились на 36% до 333,3 млрд руб. (или на 25% до 436 539 шт.). В Национальном бюро кредитных историй (НБКИ) годовой рост числа автокредитов оценили в 29%. «Автокредитование вернулось к докризисным уровням, доля кредитных автомобилей растет, - отметил генеральный директор НБКИ Александр Викулин. - В 2017 г. каждый второй автомобиль в стране был приобретен гражданами с привлечением кредитных средств». Аналитики Центрального банка объясняют это тем, что спрос на транспортные средства вырос благодаря доступным процентным ставкам по ссудам, а также активной государственной поддержке. Льготный государственный автокредит – денежный кредит на покупку нового автомобиля при действующих льготных условиях. Для того, чтобы поддерживать спрос на приобретение автомобилей, собранных в России, Государственная Дума разработала в 2009 году государственную программу кредита на автомобиль, которая действует по сегодняшний день. Стимулирующий фактор — политика Центробанка по снижению ключевой ставки. В 2017 году ставки по автокредитам на срок больше года сократились с 13,25% до 12,04%, а на срок менее года — с 11,43% до 10,10%.

По данным экспертов Национального бюро кредитных историй (НБКИ), практически в каждом российском регионе возросло количество людей, одновременно выплачивающих как минимум два кредита. Нередко второй кредит берется с целью оплатить предыдущий. Согласно статистике, за 2017 год, около 50% россиян, относящихся к категории «экономически активное население», предпочитают брать кредиты.

Представитель Сбербанка подтвердил, что число выдачи новых кредитных карт выросло, но находится «на стабильно высоком уровне». Рост кредитования населения обеспечивают в основном те люди, которые берут

кредиты, чтобы подтянуть уровень жизни, полагает главный экономист Альфа-банка Наталия Орлова: «В последние два года они больше остальных пострадали от кризиса в плане уменьшения покупательной способности».

Однако, возрастает и задолженность населения перед банками. Долг населения перед банками, т. е. сумма задолженности кредитно-финансовым институтам по потребительскому, ипотечному кредиту и другим финансовым услугам, за 2017 год превысил предельные значения. По данным ЦБ, за 2017 г. совокупные долги населения перед банками выросли на 13,2% до 12,2 трлн руб., а с начала текущего 2018 года еще увеличилась на 9,4%. Рост наблюдается во всех сегментах кредитования, в особенности – ипотечные кредиты и автокредитование.

Для исследования проблемы роста долга населения перед банками был применен парный и множественный корреляционный анализ на основе статистических данных, взятых на официальном сайте Центрального банка России и Росстата.

Исследуемый период: с2009 по 2017 год.

Исследуемые факторы (признаки):

Y – сумма долга населения перед банками за год;

X_1 – сумма ипотечных кредитов, предоставленных физическим лицам;

X_2 – объем автокредитов, предоставленных физическим лицам;

X_3 – уровень безработицы в России.

Были найдены парные и частные коэффициенты корреляции между результирующим признаком Y и каждым из факторных признаков X_1, X_2 и X_3. Получены следующие результаты:

Таблица 1

Исследуемые признаки	Парный коэффициент	Частный коэффициент
Y и X_1	0,88	0,46
Y и X_2	0,98	-0,91
Y и X_3	-0,91	0,42

Так как значения парных коэффициентов корреляции между двумя признаками показывают зависимость между этими признаками на фоне действия остальных, а частных – при исключении остальных признаков, то по результатам исследования можно сделать следующие выводы.

На увеличение суммы долга перед банками существенное влияние оказывает увеличение суммы ипотечных кредитов (0,88). Это же происходит даже при отсутствии влияния остальных признаков (0,46). Суммы по ипотекам достаточно значительные и расчетный период по недвижимому имуществу может достигать 25 лет и более.

По данным НБКИ, самая высокая долговая нагрузка в нефтяных и газовых регионах - Тюменской области, Ханты-Мансийском автономном округе, Ямало-Ненецком автономном округе и Магаданском крае. По мнению специалистов, банки охотно кредитуют жителей этих регионов, потому что у них высокие зарплаты. Задолженность российских граждан перед банками по ипотечным кредитам в ближайшие три года может увеличиться в два раза. Согласно прогнозу Агентства ипотечного жилищного кредитования (АИЖК), к 2020 году задолженность достигнет 10 трлн рублей. «С одной стороны, хорошо, что люди не боятся брать кредиты и уверены в своем завтрашнем дне, а с другой - такой излишне быстрый рост кредитования, участие людей, не умеющих рассчитывать свою нагрузку и, как следствие, с трудом расплачивающихся по обязательствам, приводят к росту просроченной задолженности», - прокомментировал исследование директор по маркетингу НБКИ Алексей Волков.

Наибольшее влияние на увеличение долга перед банками оказывает объем автокредитов, причем как в положительную, так и в отрицательную сторону. На фоне действия остальных признаков при увеличении объемов автокредитов значительно увеличивается долг населения (0,98). Однако при исключении влияния остальных признаков долг населения перед банками будет уменьшаться (-0,91). Последнее происходит благодаря тому, что при исключении из рассмотрения ипотечных кредитов и уровня безработицы, т. е. предполагая, что они находятся на постоянном уровне (не увеличиваются и не уменьшаются), население имеет возможность взять автомобиль в кредит и выплачивать стабильно проценты, так как отсутствует весомый кредит на недвижимое имущество.

При исследовании влияния уровня безработицы на долг населения появились результаты, которые позволили сделать следующие выводы. В случае, когда уровень безработицы в стране растет, увеличивается и долг населения при условии постоянных объемов ипотечного и автокредитования (0,42). Это объясняется отсутствием возможности и средств выплачивать с постоянной периодичностью сумму денежных средств в банк,

возрастает вероятность невозврата либо задержки выплаты по кредиту. Отрицательное значение парного коэффициента корреляции (- 0,91) можно объяснить, например, следующим.

С учетом того, что все парные коэффициенты корреляции между уровнем безработицы и объемами различных видов кредитования имеют отрицательные значения можно сделать вывод о том, что при увеличении уровня безработицы происходит уменьшение объемов различных кредитов, что, в свою очередь и приводит к уменьшению долга населения перед банками. Кроме этого, статистика по автокредитам и ипотеке рассчитывается на одного должника, но у одного безработного может при этом быть кредит на автомобиль и ипотека одновременно, не исключением являются случаи оформления нескольких кредитов на одного человека.

Заключение.

Исходя из результатов корреляционного анализа статистических данных, прогнозов Центрального банка и Объединенного кредитного бюро рост задолженности населения перед банками будет продолжать расти. Существуют разные точки зрения аналитиков и экспертов банков по поводу разрешения вопроса о возврате кредитов банкам. К наиболее перспективным, на взгляд авторов, следует отнести:

1. Юридические консультации от банка – кредитора перед оформлением кредита, что впоследствии способствует избеганию разногласий в правовых вопросах выплаты кредита.
2. Работы по повышению финансовой грамотности граждан. Финансовые консультации от банка – кредитора для уточнения возможности периодичности и стабильности выплат заемщика.
3. Усовершенствование программ рефинансирования для граждан, которые находятся в сложной материальной ситуации, в связи с чем покрывают один кредит другим.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральная служба государственной статистики http://www.gks.ru/
2. Объединенное кредитное бюро http://www.bki-okb.ru/
3. Официальный сайт Банка России https://www.cbr.ru/
4. Аналитический Центр по ипотечному кредитованию и секьюритизации http://rusipoteka.ru/
5. Национальное бюро кредитных историй https://www.nbki.ru/
6. Официальный сайт Альфа-банка https://alfabank.ru/press/news/2017/12/5/41861.html
7. Официальный сайт ООО «Русфинанс Банк» https://www.rusfinancebank.ru/ru/media-about.html
8. Официальный сайт AUTOSTAT.RU - статистика, исследование и анализ автомобильного рынка России. https://www.autostat.ru/

УДК 004.056.53

АРХИТЕКТУРА ЦИФРОВОЙ ЭКОНОМИКИ

Верзун Наталья Аркадьевна[1], Колбанёв Михаил Олегович[1], Шамин Алексей Анатольевич[2]
[1] Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
[2] Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия
e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, ngiei-spo@mail.ru

Аннотация. Показано, что внедрению технологий цифровой экономики все сильнее мешает противоречие между единичными и общим подходами к ее созданию. С одной стороны, можно наблюдать рост финансирования большого количества локальных задач, развития тех или иных технологий, пилотных проектов и стартапов, с другой стороны, – недостаточное внимание к развитию комплексного системного взгляда на цифровую экономику как на целостный технологический проект, использующий обобщенные и стандартизированные информационные модели и архитектуру. Предлагается стратифицированная модель цифровой экономики, призванная снять это противоречие.

Ключевые слова: информационное общество; цифровая экономика; архитектура системы; стратифицированное описание системы.

ARCHITECTURE OF THE DIGITAL ECONOMY

Verzun Natalia[1], Kolbanev Mikhail[1], Shamin Alexey[2]
[1] Saint-Petersburg State University of Economics
21 Sadovaya Str., St. Petersburg, 191023, Russia
[2] Nizhny Novgorod state University of engineering and Economics
22A Oktyabrskaya Str., Knyaginino, 606340, Russia
e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, ngiei-spo@mail.ru

Abstract. It is shown that the introduction of digital economy technologies is increasingly hampered by the contradiction between single and common approaches to its creation. On the one hand, one can observe the growth of financing of a large number of local tasks, the development of certain technologies, pilot projects and start-ups, on the other hand, insufficient attention to the development of a comprehensive systemic view of the digital economy as a holistic technological project that uses generalized and standardized information models and architecture. A stratified model of the digital economy is proposed, designed to remove this contradiction.

Keywords: information society; digital economy; system architecture; stratified description of the system.

Введение.

Новый качественный уровень информационных и коммуникационных технологий, их стандартизация и массовое внедрение обеспечивают переход к очередному этапу развития информационного общества – цифровой экономике, которая стала политической, экономической и культурной целью всех развитых стран современного мира. Построение цифровой экономики предполагает решение множества задач, возникновение которых имеет одну общую первопричину – кардинальное изменение технологий информационного взаимодействия [1]. Цель проведенного исследования – построение архитектурной модели цифровой экономики, объединяющей весь комплекс основополагающих принципов ее технологической организации, которые воплощены в наборе цифровых технологий, связей технологий друг с другом и с внешним окружением.

Обсуждение. Анализ экономической литературы по распространению термина «цифровой» – «digital» в описаниях публикаций EconLit по предметным областям JEL показывает [2], что более 80% публикаций рассматривают цифровую экономику как цифровизированные экономические отношения, позволяющие улучшить важные показатели экономической деятельности. В работах такого рода, например, [3], речь идет об увеличении числа коммерческих площадок, уменьшении размера компаний, кастомизированности, уменьшении числа посредников и издержек, и предполагается, что для получения всех этих возможностей достаточно организовать информационное взаимодействие через интернет.

В технической литературе в основном исследуются архитектуры отдельных технологий третьей платформы информатизации, и меньшее внимание уделяется вопросам их совместного использования.

В Государственной программе «Цифровая экономика России» как одно из базовых условий перехода к цифровой экономике выделяется создание информационной инфраструктуры, однако под инфраструктурой понимается лишь распространение интернет и развитие Единой сети электросвязи Российской Федерации. Конструктивную критику такого подхода можно найти в [4].

В Государственной программе РФ «Национальная технологическая инициатива» перечисляются, так называемые, сквозные технологии, необходимые для построения цифровых платформ. Это большие данные, искусственный интеллект, системы распределенного реестра, квантовые технологии, новые и портативные источники энергии, новые производственные технологии, сенсорика и компоненты робототехники, технологии беспроводной связи, технологии управления свойствами биологических объектов, нейротехнологии, технологии виртуальной и дополненной реальностей. При этом сквозные технологии перечислены как изолированные объекты, не связанные друг с другом, не ставится задача изучения их взаимозависимости на разных этапах жизненного цикла. Не дается оценка важности развития именно этих, а не других технологий, которые не упомянуты в документе, но также представляют тренд глобального технологического развития.

В отличие от этих подходов авторы предлагают исследовать цифровую экономику как большую цифровую информационную систему (БЦИС), объединяющую весь спектр технологий, необходимых для функционирования предприятий в новой цифровой среде. Это не только интернет, но и технологии построения реальных и виртуальных источников цифровых данных, систем и сетей сохранения, распространения и обработки данных, облачные, туманные и росистые вычисления, технологии создания структур и анализа данных, построения цифровых платформ и приложений, создания экосистемы цифровых платформ, цифровых рынков и моделей процессов деятельности.

Изолированное рассмотрение отдельных элементов цифровой экономики, как и отдельных технологий БЦИС, не позволяет принимать комплексные эффективные решения по её созданию. И поэтому предлагается формула: «Цифровая экономика» = «система экономических, социальных и культурных отношений» + «БЦИС». Эта формула объединяет весь спектр технологий, необходимых цифровым организациям для эффективного информационного взаимодействия – от цифровизации естественных процессов до формирования цифровых рынков.

Методология проведенного исследования использует принципы конструирования системных моделей, развиваемых при построении архитектур цифровых систем инфокоммуникаций, облачных вычислений, индустриального интернета, больших данных, наложенных сервисов и других технологий третьей платформы информатизации [5].

Использованная методология позволила разделить весь сложный процесс создания цифровой экономики на более простые части – уровни и подпроцессы, выработать общие понятия и терминологию, выделить базовую функциональность технологий для всех уровней иерархии, сформировать базовые компетенции специалистов, изучающих и реализующих разные подпроцессы, упростить задачу организации взаимодействия продуктов, реализующих подпроцессы и др.

Для того чтобы увидеть все фундаментальные технологические задачи, которые необходимо решить при построении новых моделей деятельности в условиях цифровой экономики целесообразно применять архитектурный подход. Предлагается представить архитектуру цифровой экономики в виде стратифицированной иерархической модели (см. рис.1), которая содержит две группы уровней: инфраструктурные и предметно-ориентированные.

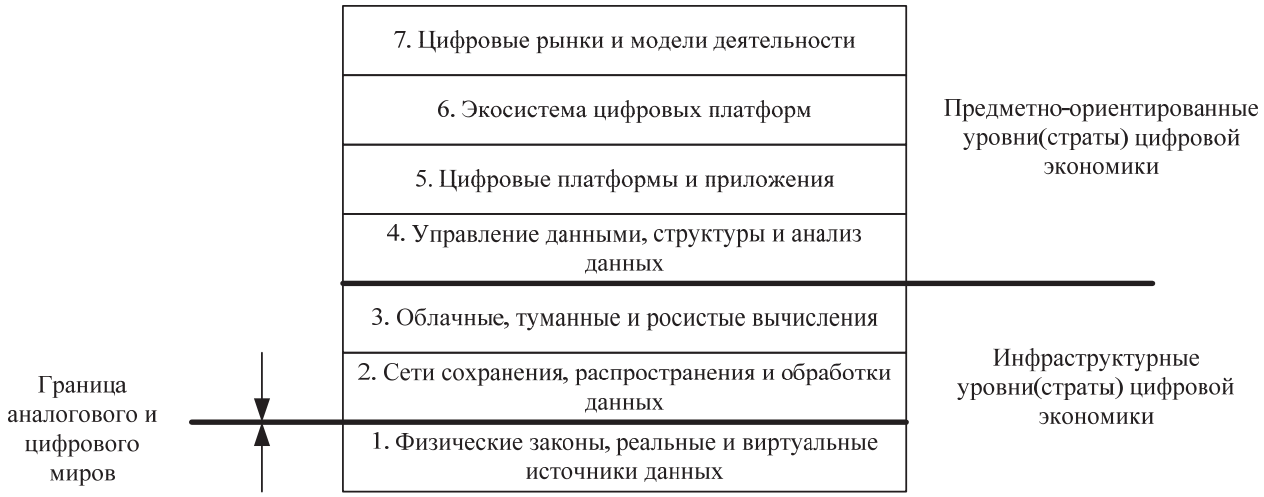


Рис.1. Стратифицированная модель цифровой экономики

К первой группе (инфраструктурные страты) следует отнести нижние три уровня предлагаемой модели:

1 уровень – технологии физической реализации информационных процессов, обеспечивающие цифровизацию естественных аналоговых процессов и представление их в виде цифровых сигналов. Они являются фундаментом цифровой экономики и развиваются благодаря фундаментальным научным исследованиям и открытию новых физических принципов представления данных. К числу технологий такого рода относятся электроника, фотоника, радиотехника, квантовые, оптические, НБИК и другие технологии [6].

2 уровень – технологии создания киберпространства для обеспечения глобального информационного взаимодействия. На этой страте создаются условия для взаимодействия источников данных во времени, в пространстве и при помощи обработки данных. Используемые для этого технологии сохранения, распространения и компьютерных вычислений вышли на новый виток развития. Их объемные характеристики измеряются в Петабайтах, Терабит/с, Петафлопсах, соответственно, и продолжают рост в соответствии с достижениями фундаментальной науки. Важными достижениями стало создание интернета вещей, дающего возможность внедрять самые разнообразные приложения [7, 8], тактильного интернета, масштабных центров обработки данных (ЦОД), суперкомпьютеров и т.п.

3 уровень – технологии вертикального распределения данных между пулом централизованных ресурсов сохранения и обработки и местами их возникновения и использования. Их главное предназначение – организация процессов предоставления услуг сохранения, распространения и обработки данных конечным пользователям. Это облачные, туманные и росистые вычисления – технологии которые объединяют в единую инфраструктуру все компьютерные системы от терминальных устройств до масштабных ЦОД, обеспечивая высокие: производительность для доставки и обработки данных с низкими задержками; устойчивость за счет резервирования и восстановления данных при системных сбоях; надежность для гарантированного сохранения данных; открытость в смысле обеспечения переносимости ПО и данных, интероперабельности и масштабируемости.

Как и в архитектурных моделях других цифровых систем [9–12], отношения соседних страт цифровой экономики характеризуются иерархической подчиненностью. Так, первая страта предоставляет страте 2 цифровые данные в определенном формате. На второй страте эти данные получают новые метаданные, определяющие их расположение в киберпространстве. Передача данных на третью страту со второй сопровождается выработкой дополнительных метаданных, связанных с характером информационных услуг, предоставляемых пользователям. Совместно технологии трех нижних страт образуют инфраструктурный технологический уровень цифровой экономики.

Ко второй группе (предметно-ориентированные страты) относятся четыре верхних уровня модели:

4 уровень – технологии управления данными, формирования логических структур данных и извлечения информации из данных. Структура данных и алгоритмы их анализа тесно связаны друг с другом, при этом:

– выбор структуры для представления больших данных является значительно более сложной задачей по сравнению с упорядочиванием малых данных. Это объясняется увеличением масштаба, числом источников данных, разным составом данных (текущие, исторические, неструктурированные, мониторинга и др.), разными форматами представления данных, не однозначной интерпретацией смыслов данных и др.;

– алгоритмы анализа структурированных данных как правило проще вычислительных алгоритмов.

Логику анализа данных легче выстроить, если данным сопоставлены подробные метаданные, характеризующие их структуру и смысл. С другой стороны, метаданные существенно увеличивают объемы хранения.

Типовыми структурами данных сегодня являются базы данных разного типа (SQL и NoSQL), хранилища и озера данных, а средствами анализа – OLAP (On-Line Analytical Processing) средства, статистические математические алгоритмы, методы DataMining и др. Особый класс задач – это анализ больших данных в реальном масштабе времени. Технологии четвертой страты придают новые системные свойства цифровым

данным, полученным от инфраструктурных уровней, добавляя к ним новые метаданные, повышающие степень организации информационных ресурсов в целом.

5 уровень – технологии создания информационного пространства для координации рыночных взаимодействий производителей и потребителей товаров и услуг. Это технологии создания цифровых платформ, которые являются основными строительными блоками для цифровой экономики. Их главные свойства: открытые защищенные интерфейсы для информационного взаимодействия с внешним окружением; предоставление виртуальных площадок для коммуникации участников рынка; сохранение, распространение и обработка огромных объемов данных; предоставление услуг клиентам, распределенным на большой территории; облачный характер услуг (XaaS – все как сервис), предоставление услуг в реальном времени по первому требованию с оплатой за реальный объем потребления; основные активы – это новые инновационные разработки и бизнес-идеи; отход от субъект-объектной концепции, интеграция материальной (предметной) и управленческой деятельностей при производстве, распределении, обмене и потреблении блага; полная автоматизация практически всех видов деятельности; принятие решений в масштабе всего предприятия-платформы и др.

Главное для платформенных технологий – это организация связей с внешним окружением, а не внутреннее устройство. Цифровые платформы являются распределенными информационными системами, управление которыми, в зависимости от метода структурирования данных на четвертой страте, может быть централизованным или децентрализованным.

6 уровень – технологии, призванные создать экосистему цифровых платформ – партнерство, обеспечивающее взаимодействие цифровых платформ на базе «цифрового кодекса», научно-технологических стандартов и гарантий безопасности [13, 14]. По современным представлениям цифровая среда должна быть подобна экологическим системам, созданным природой. Структуры экосистемы, производящие требуемые товары и услуги, формируются информационными потоками, которые циркулируют между платформами и пользователями и получают новые свойства каждый раз при достижении ими тех или иных цифровых платформ. В основе лежит три технологических принципа, поддерживаемых пятью нижележащими уровнями – сетевой, открытости технологий и открытости данных.

7 уровень – технологии цифровых рынков, представляющие собой цифровые информационные сети, в которых посредники заменены на управляющее программное обеспечение: рынки и процессы деятельности цифровой экономики. Критерии выбора рынков в России сформулированы в рамках государственной программы «Национальная технологическая инициатива» [15], где в частности отмечается следующее: рынок станет значимым и заметным в глобальном масштабе, объем составит более $100 млрд к 2035; на текущий момент рынка нет, либо на нем отсутствуют общепринятые/устоявшиеся технологические стандарты; рынок в первую очередь ориентирован на потребности людей как конечных потребителей (приоритет B2C над B2B); рынок будет представлять собой сеть, в которой посредники заменяются на управляющее программное обеспечение; рынок важен для России с точки зрения обеспечения базовых потребностей и безопасности; в России есть условия для достижения конкурентных преимуществ и занятия значимой доли рынка; в России есть технологические предприниматели с амбициями создать компании-лидеры на данном высокотехнологичном новом рынке. В настоящее время разработаны или разрабатываются дорожные карты для развития более десяти цифровых рынков [15].

Заключение.

В работе представлены следующие научные результаты:

– произведен анализ свойств и признаков цифровой экономики, который, в отличие от известных, ставит во главу угла необходимость сохранения, распространения и обработки огромного объема цифровых данных, что позволяет рассматривать цифровую экономику как большую цифровую информационную систему;

– выявлены предпосылки для архитектурного описания цифровой экономики, в основе которых лежат ее системные, информационные и технологические особенности как большой цифровой информационной системы, что позволило установить необходимость и возможность стратифицированного описания процессов информационного взаимодействия ее компонент;

– разработана архитектура цифровой экономики в виде стратифицированной модели, отличающаяся от известных моделей иерархической упорядоченностью всех необходимых процедур и технологий, что позволило отобразить последовательное изменение исходных массивов данных и метаданных на этапах и фазах реализации процессов деятельности в рамках цифровой экономики.

Методология проведенного исследования позволила, в частности:

– разделить весь сложный процесс создания цифровой экономики на более простые части – уровни и подпроцессы;

– выработать общие понятия и терминологию;

– выделить базовую функциональность технологий для всех уровней иерархии;

– сформировать базовые компетенции специалистов, изучающих и реализующих разные подпроцессы;

– упростить задачу организации взаимодействия продуктов, реализующих подпроцессы и др.

Построенная архитектура цифровой экономики является реальным инструментом, позволяющим государству и бизнесу выявить фундаментальные технологические задачи, которые необходимо решить для построения моделей деятельности в условиях цифровой экономики с учетом проблем ресурсной эффективности [16], информационно-экономической безопасности [17, 18] и требований к качеству обслуживания пользователей [19, 20].

СПИСОК ЛИТЕРАТУРЫ

1. Астахова Т. Н., Колбанёв М. О., Шамин А. А. Децентрализованная цифровая платформа сельского хозяйства // Вестник НГИЭИ. 2018. № 6 (85). С. 5−17.
2. Лычагин М.В., Лычагин А.М., Таратута В.П. Цифровой аспект в мировой экономической литературе. URL: http://inecprom.spbstu.ru/files/inprom-2017/inprom-2017.pdf.
3. Юдина Т.Н. Осмысление цифровой экономики. Теоретическая экономика, №3, 2016, С. 12–16.
4. Шнепс-Шнеппе М.А., Сухомлин В.А., Намиот Д.Е. О Программе «Цифровая экономика Российской Федерации»: как создавать информационную инфраструктуру // International Journal of Open InformationTechnologies. – 2018 – Т. 6, № 3. С. 37–47.
5. Верзун Н.А., Колбанёв М.О., Омельян А.В. Введение в инфокоммуникационные технологии и сети FUTURE NETWORKS/ учебное пособие/ Санкт-Петербургский государственный экономический университет. – 2016. – 51 с.
6. Верзун Н. А., Колбанев М. О., Цехановский В. В. Принципы построения и характеристики цифровых сетей нового поколения. СПб.: Изд-во СПбГЭТУ «ЛЭТИ». – 2017. – 212 с.
7. Быстряков Д.С., Колбанёв М.О., Цехановский В.В. Архитектура сетецентрической системы мониторинга аромобезопасности жизненного пространства // XX Международная конференция по мягким вычислениям и измерениям (SCM-2017). Сборник докладов в 2-х томах. Санкт-Петербург. 24-26 мая 2017 г. Т.2. – С. 293–296.
8. Афанасьев Д.С., Колбанёв М.О., Цехановский В.В. Физический уровень системы мониторинга аромобезопасности // XX Международная конференция по мягким вычислениям и измерениям (SCM-2017). Сборник докладов в 2-х томах. Санкт-Петербург. 24-26 мая 2017 г. Т.2. – С. 297–300.
9. Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. М.: Издательство «Мир». – 1973. – 344 с.
10. Интернет вещей // Recommendation Y. 2060. Overview of Internet of Things. ITU-T, Geneva. June 2012.
11. NIST Cloud Computing Standards Roadmap // National Institute of Standards and Technology. URL: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024.
12. Introduction to big data classification and architecture. URL: https://www.ibm.com/developerworks/library/bd-archpatterns1/index.html?S_TACT =105AGX99&S_CMP=CP.
13. Кефели И.Ф., Колбанев М.О. К вопросу о становлении науки глобальной безопасности // Геополитика и безопасность. 2017. № 4. – С. 15–21.
14. Васильев Ю.С., Кефели И.Ф., Колбанев М.О. Антропоцен и глобальная безопасность: научный прогноз В. И. Вернадского // Материалы международной научно-практической конференции «В.И. Вернадский и перспективы развития российской науки» (к 155-летию со дня рождения В.И. Вернадского), Санкт-Петербург, 12-13 марта 2018 г. / СЗИУ РАНХиГС. – СПб.: ИПЦ СЗИУ РАНХиГС. 2018. – С. 30–38.
15. Государственная программа «Национальная технологическая инициатива». URL: https://asi.ru/nti/.
16. Колбанёв М.О., Татарникова Т.М. Физические ресурсы информационных процессов и технологий // Научно-технический вестник информационных технологий, механики и оптики. Том 14, № 6. 2014. – С. 113–123.
17. Колбанёв М.О., Коршунов И.Л., Левкин И.М. Информационно-экономические угрозы и механизм их формирования//Геополитика и безопасность. – 2016. – №1 (33). – С. 85–90.
18. Кефели И. Ф., Колбанёв М. О. К вопросу о формировании теории глобальной безопасности//Геополитика и безопасность. – 2017. – №4 (40). – С. 15–21.
19. Верзун Н.А., Колбанев М.О., Советов Б.Я., Яшин А.И. Методы сбора данных с сенсорных узлов беспроводной сенсорной сети / Известия СПбГЭТУ ЛЭТИ. 2018. Т. 5. – С. 55–60.
20. Верзун Н.А., Колбанёв М.О., Омельян А.В. Регулируемый множественный доступ в беспроводной сети умных вещей / Омский научный вестник. Сер. Информатика, вычислительная техника и управление. – 2016. – No 4 (148). – С. 147–151.

УДК 330.46, 658.5.012.1, 658.511.3

ВРЕМЕННАЯ ДИАГРАММА ПОТОКА СОБЫТИЙ КАК ИНСТРУМЕНТ ОЦЕНКИ ОПЕРАЦИОННОГО РИСКА ПРЕДПРИЯТИЯ

Карасева Екатерина Ивановна
Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП)
Большая Морская ул., 67, Санкт-Петербург, 190000, Россия
e-mail: matatkakate@gmail.com

Аннотация. В статье в общих чертах излагается разработанный автором новый процессно-событийный подход для количественной оценки операционного риска в динамике и вычисления величины резервируемого капитала на предприятии реального сектора экономики. Для вычисления и анализа величины операционного риска используется логико-вероятностный метод. Автор предлагает моделировать активные процессы предприятия как цепочки событий. Логические функции строятся по возможным критическим комбинациям событий активных процессов предприятия. Вводится понятие «диаграмма Карасевой» для графического описания функционирования предприятия как потока событий.

Ключевые слова: процесс; событие; логика; вероятность; риск; управление; поток событий; диаграмма Карасевой.

TIME DIAGRAM OF EVENT FLOW AS A TOOL FOR OPERATIONAL RISK ESTIMATION IN ENTERPRISE

Karaseva Ekaterina
Saint-Petersburg State University of Aerospace Instrumentation (SUAI)
67 Bolshaya Morskaya Str., St. Petersburg, 190000, Russia
e-mail: matatkakate@gmail.com

Abstract. The paper outlines the new process-event approach developed by the author for quantitative estimation of operational risk in dynamics and calculating the amount of reserved capital in the enterprise of the real sector of the economy. To calculate and analyze the operational risk value, the logical-probabilistic method is used. Author proposes to model the active processes of the enterprise as a chain of events. Logical functions are built on the basis of possible

critical combinations of events of active enterprise processes. The concept of “Karaseva diagram” is introduced to graphically describe the functioning of an enterprise as a stream of events.

Keywords: process; event; logics; probability; risk; management; event flow; Karaseva diagram.

В мировой банковской практике управление операционным риском является ключевой и первостепенной задачей. Операционный риск проникает во все аспекты других возможных рисков, а точнее, он взаимосвязан со всеми другими типами риска (например, рыночным и кредитным рисками, а также риском ликвидности), усложняя их. В отсутствие операционных провалов все другие типы риска значительно менее важны. Задача оценки и управления операционным риском является одной из самых сложных в риск-менеджменте [1-3].

ЦБ РФ дает следующее определение: «операционный риск — это риск возникновения убытков в результате несоответствия характеру и масштабам деятельности кредитной организации и (или) требованиям действующего законодательства внутренних порядков и процедур проведения банковских операций и других сделок, их нарушения служащими кредитной организации и (или) иными лицами (вследствие непреднамеренных или умышленных действий или бездействия), несоразмерности (недостаточности) функциональных возможностей (характеристик) применяемых кредитной организацией информационных, технологических и других систем и (или) их отказов (нарушений функционирования), а также в результате воздействия внешних событий» [4].

На самом деле, операционный риск характерен не только для банков. Операционный риск является сложным системным явлением, присущим всем сложным социально-экономическим системам. Это нефинансовый риск и проявляется в деятельности любого субъекта экономики – коммерческого предприятия, инвестиционной компании, индустриального предприятия, социального учреждения, учреждений исполнительной и законодательной власти, армии.

Операционный риск проявляется прежде всего в событиях: ошибки сотрудников предприятия, отказы информационных систем, политические события, вооруженные нападения, явления природного характера. Поскольку события имеют разную природу, то возникают сложности в формализованном описании и моделировании операционного риска. В работе [5], например, операционный риск предприятия сводится лишь к событиям, связанным с человеческим фактором.

На наш взгляд, для предприятия реального сектора экономики операционный риск выражается в нежелательных событиях (внешних или внутренних), ведущих к невыполнению отдельно взятой операции или процедуры, которая является неделимым действием.

Ввиду отсутствия стандартов, регуляторных документов и четких методов для оценки операционного риска на коммерческих предприятиях реального сектора экономики представляется целесообразным строить новую методику на основе процессного подхода к управлению [6] с использованием событийной онтологии. Основы событийного подхода к описанию явлений и процессов были положены в трудах известных философов Л. Витгенштейна [7] и Б. Рассела [8] и развиты в работе [9] как субъектно-событийный подход.

В субъектно-событийном подходе основным и единственным элементом описания систем является событие: предприятие представляется как поток событий, выполняемых субъектами над объектами, причем сами субъекты и объекты фиксируются в системе как множества связанных с ними событий, большинство из которых совершается в процессе функционирования предприятия, а часть фиксируется на момент включения объектов и субъектов в систему.

В [10] авторы субъектно-событийного подхода выделяют три важнейших принципа:

1. Принцип выделения событий. Для анализа функционирования сложной системы нет необходимости фиксировать каждое событие на уровне технологических процессов. Выделяемое событие должно соответствовать трем условиям:

- событие выполняется или регистрируется одним из субъектов системы;
- событие выполняется над одним из объектов системы;
- факт наличия (или отсутствия) события является условием для выполнения события другим субъектом или этим же субъектом, но с другим объектом.

2. Принцип унификации: все субъекты и все объекты, входящие в предприятие, исчерпывающе описываются как множества событий. В событийном подходе любое утверждение о любом объекте оформляется как утверждение о событии, фиксируемом или инициируемом конкретным субъектом. Сказанное об объектах в рамках событийного подхода можно сформулировать и в терминах данных: любые данные в субъектно-событийном подходе порождаются событиями и записываются как события. Данные могут как поступать на вход системы (входящие ресурсы, условия заказа), так и генерироваться в системе (модификация ресурсов) – в любом случае они описываются как события приписывания предиката объекту, выполненные конкретным субъектом.

3. Принцип релятивности. Каждый объект включается в действия субъекта с тем набором параметров, которые различимы в этом действии. Отношения между субъектами фиксируются также только в той степени, насколько пересекаются их событийные множества: субъекты связаны с одним объектом, включены в одно действие. Изменение состояния объектов носит относительный, субъектный характер. Если какой-либо субъект не различил событие изменения, то для него объект не изменил состояние. Событийный подход снимает проблему однозначности классификации объектов: ресурсов, артефактов, документов, продуктов и пр. Поскольку все различаемые субъектами объекты мыслятся как множества событий, то и нет необходимости

абсолютного закрепления их типов: в зависимости от уровня и роли субъекта из общего множества событий, связанных с некоторым объектом, могут быть выделены разные подмножества, которые будут фиксироваться как разные типы. Отмеченный релятивный принцип в определении объектов и субъектов важен как для унификации и минимизации описания, так и для оптимизации отношений субъектов и объектов. А самое главное, он позволяет продуцировать и анализировать множество существенно не совпадающих, однако, согласованных на нижнем уровне (на уровне потока событий) описаний системы, выполненных с позиции различных субъектов.

Мы предлагаем новый процессно-событийный подход, в основе которого лежит концепция выделения цепочек значимых элементарных событий из процессов предприятия. Для определения величины операционного риска предприятия используется логико-вероятностный метод, ранее примененный автором для решения задачи оценки, анализа и управления операционным риском в соответствии со стандартом Базель II [11, 12].

Под цепочкой событий процесса мы имеем в виду последовательность случайных событий, связанных с успешным завершением действия (функции, процедуры, операции). В нашей трактовке количество и последовательность событий в цепочке соответствует количеству и последовательности действий в процессе. Таким образом, процесс рассматривается как последовательность неслучайных действий, результат каждого из которых представляет собой случайное событие.

Процессы могут выполняться как последовательно (когда выход одного процесса является входом для другого), так и параллельно.

При процессно-событийном подходе мы сначала определяем рабочие процессы и составляем цепочки событий. При этом можно использовать составленные ранее диаграммы бизнес-процессов в нотациях EPC, BPMIN 2.0. Затем отсекаем принципиально невозможные множества (комбинации несовместных событий) цепочек параллельных и последовательных процессов.

Мы рассматриваем предприятие как цельную структуру, распределенную во времени, которая характеризуется потоком событий. Множество всех событий, происходящих на предприятии, представляет собой полное описание предприятия или пространство состояний предприятия. Поток событий иллюстрирует временная диаграмма Карасевой (рис. 1) [13].

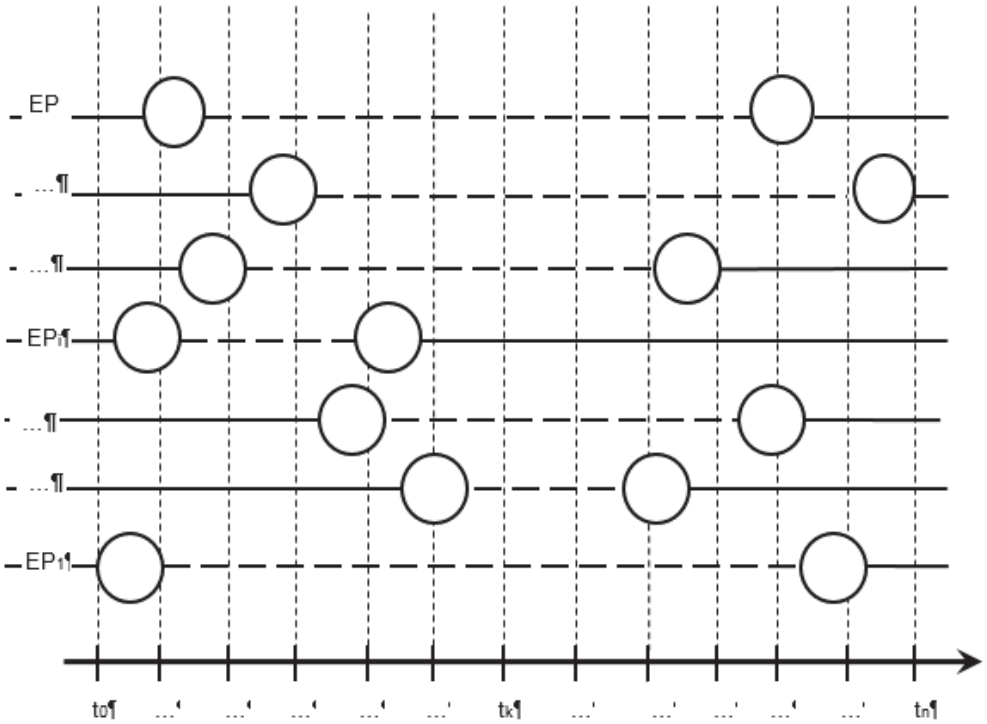


Рис. 1. Временная диаграмма событий, иллюстрирующая поток событий предприятия. Карасева Е.И. ©

Диаграмма представляет собой отображение потока событий предприятия на временной оси. Поток событий формируется активными процессами предприятия. Совокупность событий всех процессов St в момент времени t_k, k = 1, …, n на срезе диаграммы определяет величину $P(Z_{OR})$ – операционный риск предприятия. Временная диаграмма Е.И. Карасевой демонстрирует нам теоретическую возможность рассчитать величину операционного риска предприятия в любой момент времени. В работе [13] приведен пример расчета на реальных данных предприятия строительной отрасли.

Совокупность всех процессов EP_i предприятия в виде цепочек событий образует непустое конечное множество B, $EP_i \in B$, i = 1, …, m, где m – общее число выделенных процессов предприятия. Часть процессов этого множества происходят параллельно во времени, поэтому в каждый момент времени t на срезе временной диаграммы мы имеем некоторое множество событий St, состоящее из текущих, нереализованных на момент времени t, событий цепочек EP_i, i = 1,…, m.

Элементарное событие X_i заключается в успешном завершении i-действия (i-операции, i-функции), либо само по себе является событием процесса. Событие X_1 является инициирующим событием процесса, вероятность его возникновения определяет вероятность инициализации всего процесса. Событие X_9 является завершающим событием, его вероятность есть вероятность успешного завершения всего процесса.

Как упоминалось выше, каждое элементарное событие X_i мы рассматриваем как случайное, которому соответствует своя вероятность реализации $P(X_i)$. Событие X_i может не наступить по различным причинам.

Вероятность нереализации события X_i равна $Q(X_i) = 1 – P(X_i)$ и эту вероятность мы считаем величиной текущего операционного риска на данной цепочке событий (процессе).

Присвоим событиям из множества S_t логические переменные Z_m, m = 1, …, n. Логическая переменная Z_m может принять значение 1 (событие произошло) с вероятностью $P(Z_m = 1)$, или значение 0 (не произошло) с вероятностью $Q(Z_m = 0) = 1 - P(Z_m = 1)$. В момент времени t любое событие Z_m из множества S_t , либо сразу несколько событий, либо все события могут не произойти.

Логическая функция интегрированного операционного риска банка запишется в следующем виде:

$$Z_{OR} = \overline{Z}_1 \vee \overline{Z}_2 \vee \ldots \vee \overline{Z}_n \qquad (1)$$

Тогда общий интегрированный операционный риск банка $P(Z_{or})$ можно вычислить из выражения (вероятностной функции) [14]:

$$P(Z_{or}) = 1 – P(Z_1)P(Z_2) \ldots P(Z_n) \ . \qquad (2)$$

Величина $P(Z_{or})$ по сути является вероятностью нереализации любого из событий множества St. Теперь, зная величину $P(Z_{or})$ можно вычислить размер резервируемого капитала из выражения:

$$RC = P(Z_{or})\ L\ , \qquad (3)$$

где L - средняя величина убытков предприятия вследствие событий операционного риска за предыдущие три года.

Величина $P(Z_{OR})$ может служить текущим показателем надежности предприятия, поскольку является по существу сверткой остальных рисков ввиду учета таковых в вероятностях элементарных событий процессов.

По аналогии с методом, описанном в работе [12], мы вводим понятия верхней и нижней границ операционного риска, соответственно верхней и нижней границ резервирования капитала. Верхнюю границу $P(Z_{OR})up$ определяет максимальная величина операционного риска, полученная на множествах St, нижнюю границу определяет минимальная величина $P(Z_{OR})down$.

Расчет верхней и нижней границ резервирования капитала осуществляется по формулам:

$$RCup = P(Z_{OR})_{up}\ L\ ,$$

$$RCdown = P(Z_{OR})_{down}\ L\ , \qquad (4)$$

Выбор величины резервирования определяется текущей экономической и политической ситуацией, величиной основных рыночных индексов, опытом риск-менеджера и полнотой имеющейся у него информации.

На практике, конечно, поток событий может быть любым, как и количество активных процессов в любой момент времени (вплоть до одного активного процесса). Нам не нужно затрачивать усилия, моделируя все возможные комбинации активных процессов. Прежде всего, нас интересует такие множества St, при котором возможные комбинации событий приведут к максимальному операционному риску. При этом следует заранее определить и игнорировать комбинации несовместных событий.

Задача управления операционным риском с использованием процессно-событийного подхода сводится к определению всех возможных критических комбинаций событий, при которых будут максимальными величины операционного риска и убытков.

Определив критические комбинации, мы сможем вычислить вклады отдельных элементарных событий в операционный риск, а также планировать деятельность предприятия таким образом, чтобы избежать появления критических комбинаций.

Роль предлагаемого процессно-событийного подхода будет неуклонно возрастать.

Распространение информационных систем управления бизнес-процессами (BPM), систем управления потоками работ (WFM), систем ERP II и систем обработки прецедентов (Case Handling) дало возможность фиксировать отдельные события и вести журналы событий в процессе функционирования предприятия. Эти журналы (или протоколы) оказались настолько полезны для анализа и принятия управленческих решений, что стали применяться и в других областях, например, в транспорте – сейчас многие автомобили и общественный транспорт оснащены информационной системой с журналом фиксации событий.

Перед менеджерами стоит задача «извлекать» процессы из журналов событий функционирования информационных систем, организаций и предприятий. Задача особенно актуальна в тех случаях, когда формальное описание или модель системы отсутствуют или имеют низкое соответствие реальному поведению системы, то есть в 98% случаев. Для решения этой задачи активно разрабатываются технологии Process Mining [15], позволяющие извлечь из журнала событий модель процесса, проверить ее соответствие на статистике

последующих событий, и выполнить ее усовершенствование, если имеется расхождение между данными модели и процесса.

Вся деятельность предприятия, использующая ресурсы, рассматривается как совокупность процессов [6]. Каждый процесс состоит из некоторой последовательности действий. Часто выход одного процесса образует непосредственно вход следующего. Преимущество процессного подхода состоит в непрерывности управления, которое он обеспечивает на стыке отдельных процессов в рамках их системы, а также при различной комбинации процессов и их взаимодействии.

Для построения моделей процессов существует несколько наборов условных графических обозначений (нотаций). Описание и анализ процессов предприятия сводится к имитационному моделированию при помощи нотаций и блок-схем, это позволяет оптимизировать процессы, но не позволяет решить задачу оценки операционного риска предприятия.

Существующие технологии управления операционным риском часто упускают из вида главный факт: операционный риск – это нефинансовый риск и проявляется в отдельных событиях.

Автором была учтена эта особенность и предложен процессно-событийный подход для количественной оценки операционного риска. По сути, процессно-событийный подход представляет собой развитие традиционного процессного подхода к управлению предприятием. Переход к событийному описанию процессов позволяет практически решить сложную трудноформализуемую задачу количественной оценки операционного риска и резервирования капитала.

На текущем этапе разработки новой методики уже обозначилось несколько преимуществ процессно-событийного подхода:

1. Для описания процессов функционирования предприятия в процессно-событийном подходе требуется меньше переменных, чем при традиционном процессном подходе с использованием нотаций, что продемонстрировано на практическом примере [13].

2. Моделирование процессов посредством цепочек событий позволяет рассчитать величину операционного риска предприятия в момент времени t, выявить наиболее опасные комбинации событий и рассчитать величину резервируемого капитала.

3. Процессно-событийный подход позволяет рассчитать величину операционного риска не только как вероятность совокупности внутренних событий процессов, но и с учетом внешних событий (изменения законодательства, стихийного бедствия, вооруженного ограбления и т.п.). Это реализуется путем добавления соответствующих логических переменных в формулу (1). Однако, есть основания полагать, что при определении вероятностей $P(X_{i,\ m})$, m = 1, …, n, согласно протоколу событий (статистическим данным), влияние внешних факторов уже учитывается в величинах этих вероятностей.

4. Процессно-событийный подход использует простые и прозрачные формулы для расчета величины операционного риска и величины резервируемого капитала для покрытия убытков.

Процессно-событийному подходу также присущи и недостатки:

1. Отсутствие четких рекомендаций по выделению событий. Мы рекомендуем выделять элементарные события, имеющие принципиальное влияние на логику выполнения процесса и которые можно регистрировать.

2. Могут возникнуть сложности с определением величин вероятностей событий $P(X_{i,\ m})$. В случае отсутствия статистики приходится применять экспертные методы, что снижает достоверность результатов.

3. Процессно-событийный подход требует наличия определенного уровня знаний и компетенции у специалиста. Специалисту необходим некоторый предварительный практический опыт декомпозиции процессов и выделения элементарных событий.

СПИСОК ЛИТЕРАТУРЫ

1. Kaspereit T., Lopatta K., Pakhchanyan S., Prokop J. Systemic operational risk / Journal of Risk Finance. – Vol. 18, Issue 3. – 2017. – pp. 252-262.
2. McKim V.L. Operational risk assessment / Journal of Business Continuity & Emergency Planning. – Vol. 10, Issue 4. – Summer, 2017. – pp. 339-352.
3. Panjer H.H. Operational Risk: Modeling Analytics. – Wiley, 2006. – 448 p.
4. 2. Письмо Банка России от 24 мая 2005 г. № 76-Т «Об организации управления операционным риском в кредитных организациях»
5. Быкова И.В. Операционные риски предприятия: понятие, источники, влияние человеческого фактора // Российское предпринимательство. – 2011. – Том 12. – № 11. – С. 68-73.
6. Хамер М., Чампи Д. Ренжиниринг корпорации. Манифест революции в бизнесе. М.: Манн, Иванов и Фербер, 2007. – 288 с.
7. Витгенштейн Л. Логико-философский трактат. Философские работы. Пер. с нем. М. С. Козловой. – М.: Гнозис, 1994. – Ч.1.
8. Рассел Б. Философия логического атомизма. Библиотека аналитической философии. – Томск: Водолей, 1999. – 192 с.
9. Болдачев А., Шумаков А. О принципиально новом, субъектно-событийном подходе к моделированию бизнес-систем / [Электронный ресурс] // Режим доступа: http://www.rsci.ru/rt/researches/236426.php, дата обращения: 15.07.2018, 11.50.
10. Болдачев А. Субъектно-событийный подход к моделированию сложных систем.[Электронный ресурс] // Режим доступа: https://habrahabr.ru/post/256509/, дата обращения: 15.07.2018, 13.36.
11. Карасева Е.И. Логико-вероятностная модель для оценки операционного риска банка и резервирования капитала. Проблемы анализа риска. Том 9. – 2012. – № 2. – С. 24-34.
12. Karaseva E. Ability of Logical and Probabilistic Model for Operational Risk Management.Reliability: Theory & Applications – N 3 (42), Volume 11. – September, 2016. – pp 23-32.
13. Карасева Е. И., Карасев В. В. Процессно-событийный подход для оценки операционного риска предприятия реального сектора экономики. Анализ, моделирование, управление, развитие социально-экономических систем: сборник научных трудов XII Международной школы-симпозиума АМУР-2018, Симферополь-Судак, 14-27 сентября 2018 / Под общей редакцией А. В. Сигала. – Симферополь: ИП Корниенко А. А., 2018. - с. 199-207.
14. Solozhentsev E.D. The Management of Socioeconomic Safety / Solozhentsev E.D. –Cambridge Scholars Publishing, 2017. – 255 p.
15. Wil M.P. van der Aalst. Process Mining: Discovery, Conformance and Enhancement of Business Processes. – Springer-Verlag Berlin Heidelberg, 2011. – 352 p.

http://spoisu.ru

УДК 681.5

ЭФФЕКТИВНОСТЬ УПРАВЛЕНЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Лукьянова Людмила Михайловна
ФГБОУ ВО «Калининградский государственный технический университет»
Советский пр., 1, Калининград, 236022, Россия
e-mail: llm_llm@mail.ru

Аннотация. Обсуждается проблема оценивания эффективности операторской деятельности в автоматизированных информационных системах. Обосновываются две группы частных показателей эффективности операторской деятельности – работоспособность и расход ресурсов человека. Приводятся результаты автоматизированного оценивания уровней работоспособности и утомления человека, осуществляющего деятельность в условиях автоматизированных информационных систем.

Ключевые слова: информационная система; операторская деятельность; эффективность, оценки

EFFICIENCY OF ACTIVITIES IN AUTOMATED INFORMATION SYSTEMS

Lukyanova Lyudmila
Kaliningrad State Technical University
1 Sovietsky Av., Kaliningrad, 236022, Russia
e-mail: llm_llm@mail.ru

Abstract. The problem of effectiveness of human activity in automated information system (AIS) is discussed. The concept of «activities» and its semantic field, integral and partial indicators of the effectiveness of human activity in automated information systems are considered. A possible approach to assessing the effectiveness of human activity in automated information system and the software for monitoring and analyzing its performance and fatigue are discussed.

Keywords: information system; human activity; effectiveness; indicators

Введение и постановка проблемы.

Теория эффективности деятельности, как и теория деятельности не является завершенной, и в настоящее время ее разработка продолжается [1, 2].

Деятельность человека как форму специфической, ориентируемой целями, субъектно-объектной активности можно рассматривать на двух уровнях. Низкоуровневая деятельность подобна активности целенаправленной системы (например, компьютерной программы) и реализуется в процессах, направляемых внешними целями. Высокоуровневая деятельность человека как целеустремленной системы [3] сопряжена с целеполаганием и реализуется в процессах, направляемых внешними целями, но управляемых его внутренними целями.

В формализованной теории эффективности целенаправленных процессов [4] определены критерии и частные показатели эффективности: результативность, ресурсоемкость, оперативность. В случае низкоуровневой деятельности оценка эффективности путем вычисления указанных показателей не всегда тривиальная, но обычно решаемая задача. В случае высокоуровневой деятельности аналогичное оценивание эффективности даже при превосходных значениях результативности, ресурсоемкости, оперативности оказывается весьма приблизительным, что связано с игнорированием расхода ресурсов организма и трудностей их прогнозирования.

Новые подходы к оценке эффективности деятельности (в том числе предложенные в работах [1, 2, 4]) определяют различные перечни частных показателей эффективности (например, KPI – Key Performance Indicators) и соответствующие критерии, однако это не решает указанной проблемы. Российский стандарт в данной проблемной области отсутствует, что также не способствует снижению остроты данной проблемы при построении информационного общества с его требованием тотальной автоматизации процессов сбора, переработки и своевременной доставки достоверных сведений (данных, информации), необходимых и достаточных для эффективного решения соответствующих задач, прежде всего, задач отечественной экономики.

Оценивание эффективности деятельности человека как компонента автоматизированной информационной системы (АИС), представляющей собой вариант целостности и единства целеустремленной (человек) и целенаправленной (машина, или аппаратно-программно-информационный комплекс АИС) систем – еще более сложная задача. Сложность обусловлена недостаточной изученностью системных свойств человека и характеристик его психических механизмов, зависящих не только от генетических особенностей, но также и от эргономичности автоматизированного рабочего места, от навязываемого машиной ритма работы, порой монотонного, изматывающего и, как правило, не совпадающего с биологическим. Вместе с выдвижением и достижением собственных (внутренних) целей это может привести к чрезмерным затратам ресурсов организма, негативным психофизиологическим состояниям, переутомлению и, в итоге, не только существенно снизить эффективность деятельности, но и ухудшить здоровье человека.

Важность решения поставленной проблемы в информационном обществе делает актуальным уточнение частных показателей эффективности операторской деятельности и автоматизированный анализ их значений.

В докладе излагается подход к оцениванию эффективности операторской деятельности в АИС и реализующее его программное средство контроля и анализа уровней работоспособности и утомления человека.

Оценка эффективности операторской деятельности в АИС.

Понятие операторской деятельности и его семантическое поле. В работе [5] предложены наиболее общие классы деятельности: преобразовательная – с изменением объекта; познавательная – выработка знаний об объекте; ценностно-ориентационная – ценностное оценивание объекта (в частности, в процессе целеполагания); коммуникативная (коллективная деятельность, взаимосодействие).

В соответствии с классификацией целей [6] осуществлена систематизация видов деятельности, полезная для практического использования. Основным классам целей поставлены в соответствие следующие виды деятельности: политическая, социальная, правовая, научно-техническая, финансовая, экономическая, управленческая, производственная/хозяйственная, экологическая, а вспомогательным – дополнительные характеристики указанных видов: глобальная – локальная; главная – неглавная; постоянная – временная; сложная – простая; регламентированная – нерегламентированная.

При оценивании эффективности деятельности важно уточнить соотношение понятий «деятельность», «действие», «операция». Деятельность обеспечивает достижение конечной цели, а действие является элементом деятельности, обеспечивающим достижение промежуточной цели. Операция – это действие вместе со способом и средствами его осуществления (по сути, операция определяет технологию реализации действия). Очевидно, что понятие «действие» имеет бóльший (чем понятие «операция») логический объем, но меньшее логическое содержание (менее информативно согласно закону обратного отношения).

В АИС связи человека с объектом деятельности осуществляются опосредованно, с помощью системы воспроизведения/отображения информации (СВИ/СОИ) и пульта управления. Такую деятельность называют операторской, и в качестве еще одной характерной черты указывают на два ее этапа: восполнение человеком дефицита информации (данных и знаний) об объекте (информационный вход) и «обслуживание» объекта (в простейшем случае моторный выход).

По степени сложности входной информации и методов ее обработки человеком, а также по времени «обслуживания» выделяют два уровня операторской деятельности: I – по типу «стимул – реакция» (характеризуется практически одномоментным приемом информации и немедленным «обслуживанием»), II – с подготовкой и принятием решений (характеризуется временем приема и переработки информации и отсроченным «обслуживанием»).

Классификация операторской деятельности по степени структурированности решаемых задач и времени «обслуживания» определила следующие ее классы [7]: оператор-технолог; оператор-наблюдатель; член оперативного состава; член управленческого персонала.

Деятельность каждого класса характеризуется собственным перечнем показателей работоспособности человека (временных, скоростных, точностных, надежностных, объема памяти, качества внимания и др.) и их нормативными значениями (диапазонами значений), которые зависят от содержания деятельности и условий ее реализации. Оператор-технолог реализует операторскую деятельность I-го уровня по типу сенсомоторных реакций. В несколько меньшей степени I-й уровень характерен для оператора-наблюдателя, в гораздо меньшей – для оперативного состава. Управленческий персонал реализует операторскую деятельность II-го уровня.

В операторской деятельности любого класса интегрированы общие классы деятельности: оператор познает объект, оценивает его состояние и осуществляет целеполагание, преобразует объект, связывается с другими операторами. В то же время вес познавательных, ценностно-ориентационных, преобразовательных и коммуникативных действий и средств их реализации в разных классах операторской деятельности различен. В том числе и поэтому различны требования к временным, скоростным и другим характеристикам оператора-технолога, оператора-наблюдателя, члена оперативного состава или управленческого персонала.

Частные оценки эффективности операторской деятельности. С учетом того, что операторская деятельность реализуется разными совокупностями действий, а действие – включается в разные классы деятельности и выполняется различными способами с помощью разных средств, при принятии решений по действиям руководствуются критерием эффективности деятельности, а при принятии решений по операциям – критерием эффективности действий.

Основывающиеся на схожих принципах и пересекающихся группах частных показателей подходы к определению эффективности операторской деятельности [1, 2, 6-12] по разным причинам, указанным, например, в работе [2], до сих пор не нашли широкого применения. Не противореча их общим совместно с работой [3] положениям, под эффективностью операторской деятельности будем понимать интегративное свойство, зависящее от следующих двух взаимосвязанных комплексных свойств, оцениваемых соответствующими частными показателями:

1) работоспособность, оцениваемая посредством временных, скоростных, точностных и надежностных показателей [9] (динамика уровней данного свойства в течение рабочего дня проиллюстрирована на рис. 1, заимствованном из работы [12]);

2) расход психических ресурсов, определяемый с помощью комплекса психометрических методик, оценивающих уровни характеристик восприятия, памяти, мышления человека и т. д. и допустимые значения соответствующих показателей.

Поскольку жесткие требования к временным и скоростным характеристикам оператора-технолога, оператора-наблюдателя и члена оперативного состава могут привести к большому расходу психических ресурсов, сильному утомлению и, как следствие, к снижению работоспособности: увеличению времени реакции; уменьшению пропускной способности; сужению объема внимания; затруднению запоминания и сохранения

информации, извлечения знаний из памяти, – целесообразно оценивать и анализировать уровни работоспособности и утомления не менее четырех и двух раз соответственно в течение рабочего дня.

Для тестирования указанных частных показателей разработано встраиваемое в автоматизированное рабочее место программное средство «Эффективность операторской деятельности»(Разработка данного программного средства, реализующего оценивание временных, скоростных, точностных характеристик человека и затрат психофизиологических ресурсов на восприятие, память и мышление, осуществлена студентом КГТУ Ю.И. Финченко под руководством автора статьи.), контролирующее динамику изменения значений данных показателей и, в случае их приближения к пороговым, вырабатывающее рекомендации, следование которым позволяет упредить нежелательный тренд, снизить расход психических ресурсов и, в итоге, обеспечить требуемую эффективность автоматизированной деятельности.

Адекватных моделей переработки человеком всех возможных форм сообщений от машинного компонента АИС в настоящее время не существует. Нет и единой гипотезы о структуре памяти человека и механизмов работы с нею. В связи с этим наиболее подходящими считаются модели, ориентированные на контроль тех механизмов, которые, влияя на успешность операторской деятельности, испытывают наибольшую нагрузку при ее реализации.

Упомянутое программное средство ориентировано на оператора, перерабатывающего преимущественно буквенно-цифровые сообщения. Контроль уровня и динамики работоспособности осуществляется до четырех раз за рабочий период. При этом измеряются временные/скоростные/точностные/надежностные характеристики сенсомоторных реакций, элементарного кодирования (фигуры, экранного окна, акустического сигнала – цифрой), принятия (элементарного) дедуктивного решения. Контроль уровня и динамики утомления осуществляется дважды в начале и в конце рабочего периода с использованием до шести психометрических методик [12]: «Поиск сигнала в шуме», «Опознание», «Полное воспроизведение», «Определение отсутствующего знака», «Составление слов», «Воспроизведение буквосочетаний».

В методиках использована модель переработки человеком буквенно-цифровых сообщений, включающая:

– сенсорную память (СП), характеризуемую объемом (числом знаков, воспроизводимых немедленно после их однократного предъявления) и временем сохранения знаков (до секунды): иконическую СП при зрительном восприятии, эхоическую СП – при слуховом;

– кратковременную вербально-акустическую память (ВАП), характеризуемую хранением 7±2 оперативных единиц восприятия (семантически целостные образования) в течение десятков секунд, минут и даже часов;

– долговременную семантическую память (СемП);

– механизм перевода из СП в ВАП путем кодирования элементов СП (отдельных знаков) в словесно-акустическую форму и частичного осмысления машинного стимула на основе СемП;

– механизм повторения машинного стимула, обеспечивающий с помощью СемП установление его смысла (информационный вход человека) и выработку, совместно с механизмом активных преобразований полученной информации, ответа (моторный выход человека).

В случае операторской деятельности третьего и особенно четвертого классов при получении информации (новых сведений) механизм активных преобразований обеспечивают модификацию СемП: дополняет, удаляет или исправляет содержащиеся в СемП знания человека о мире.

1 – период врабатываемости;
2 – период оптимальной работоспособности;
3 – период полной компенсации;
4 – период неустойчивой компенсации;
5 – конечный порыв;
6 – прогрессирующее снижение продуктивности.

Рис. 1. Динамика работоспособности человека

http://spoisu.ru

Результаты автоматизированного оценивания работоспособности (временных характеристик) и утомления **(**процента правильных ответов (ППО) по методикам «Поиск сигнала в шуме» и «Опознание»**)** студента по направлению бакалавриата «Информатика и вычислительная техника» при выполнении четырехчасовой лабораторной работы «Исследование временных характеристик человекомашинного взаимодействия в АИС» по дисциплине «Человекомашинное взаимодействие» приведены в приложении. Процент правильных ответов до начала основных экспериментов (рис. 2, 3) показывает практически нулевой уровень утомления. Анализ результатов ряда основных экспериментов показал допустимую динамику увеличения времени ответов оператора (рис. 4–7). По завершению работы (рис. 8, 9) процент правильных ответов изменился во 2-4 позициях (перевернутые V-образные кривые), но также находится в допустимых пределах [12], так что его деятельность может быть охарактеризована как продуктивная (см. рис. 1).

Результаты автоматизированной оценки временных и точностных показателей человека.

Примеры двух (из шести) видеограмм с результатами оценивания ППО, характеризующего уровень утомления человека в начале рабочего периода, приведены на рис. 2, 3.

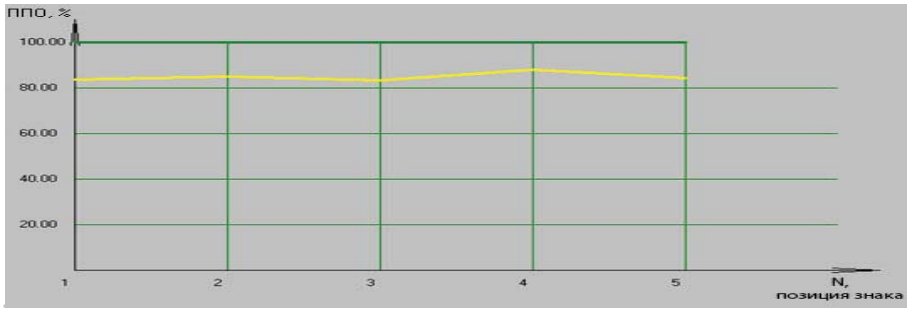


Рис. 2. Результат начального замера по методике "Поиск сигнала в шуме"

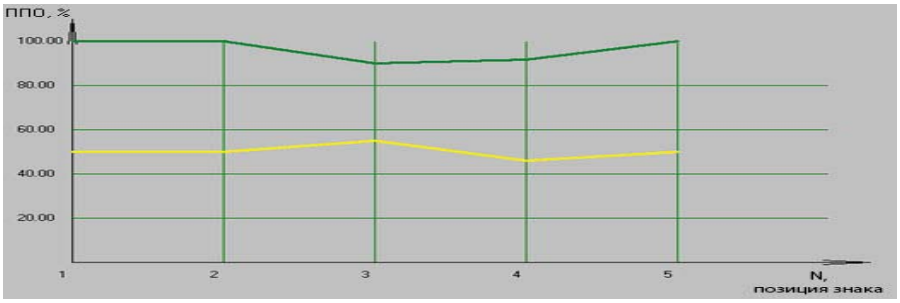


Рис. 3. Результат начального замера по методике «Опознание»

Примеры четырех (из десяти) видеограмм с результатами оценивания времени «ответов» человека-оператора приведены на рис. 4–7. Использованные в них условные обозначения:

T – цикл сенсомоторной реакции;

t_1 – время формирования машиной выходного сообщения;

$t_{2.1}$ – время обнаружения человеком выходного сообщения;

$t_{2.2}$ – время идентификации и интерпретации человеком номера окна;

$t_{2.3}$ – время идентификации и интерпретации человеком знака/фигуры;

$t_{код}$ – время кодирования человеком выведенной на экран фигуры;

$t_{3.1}$ – время ввода человеком номера окна; $t_{3.2}$ – время ввода человеком знака;

t_4 – время обработки машиной входного сообщения человека;

Y – среднее время; Y_{min} /Y_{max} – минимальное/максимальное значение среднего времени.

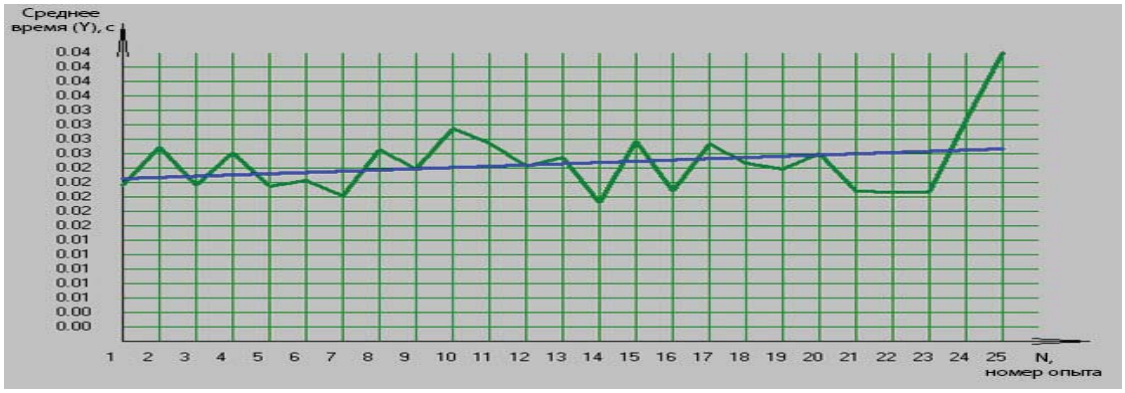


Рис. 4. Ввод цифр из множества {1, 2, 3}

$Y_{min} = 0.02375$; $Y_{max} = 0.046$; $Y = 0.034875$; $T = t_1 + t_{2.1} + t_{2.3} + t_{3.2} + t_4$.

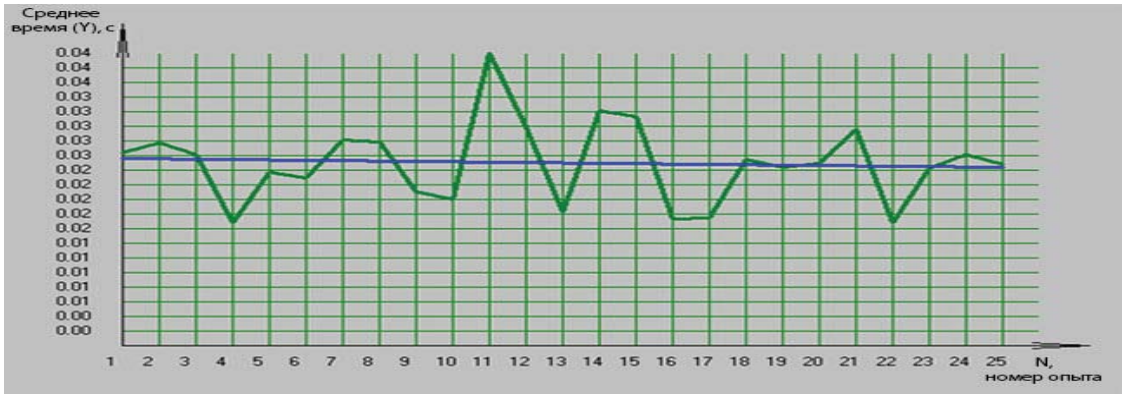


Рис. 5. Ввод букв из множества {a, b, c}

$Y_{min} = 0.021$; $Y_{max} = 0.044$; $Y = 0.0325$; $T = t_1 + t_{2.1} + t_{2.3} + t_{3.2} + t_4$.

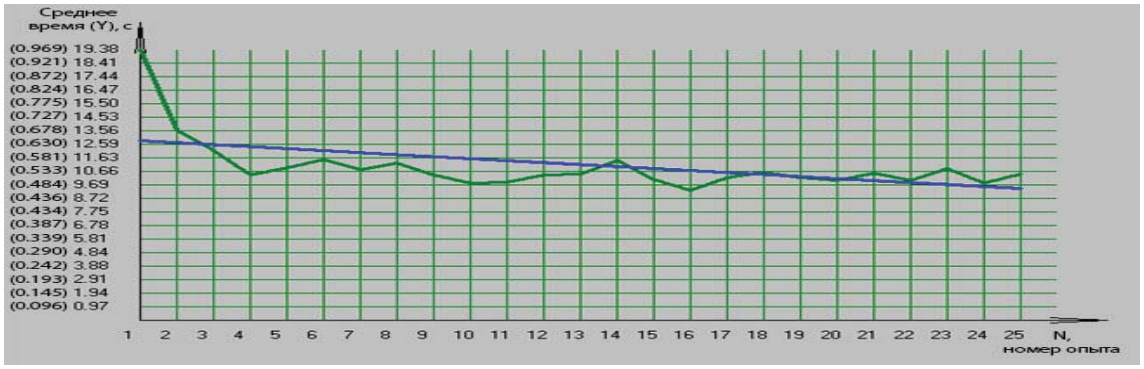


Рис. 6. Ввод фигур из множества {квадрат, треугольник, круг}

$Y_{min} = 0.472$; $Y_{max} = 0.969$; $Y = 0.6$; $t_{код} = 0.6 - 0.034875 = 0.565125$; $T = t_1 + t_{2.1} + t_{2.3} + t_{код} + t_{3.2} + t_4$.

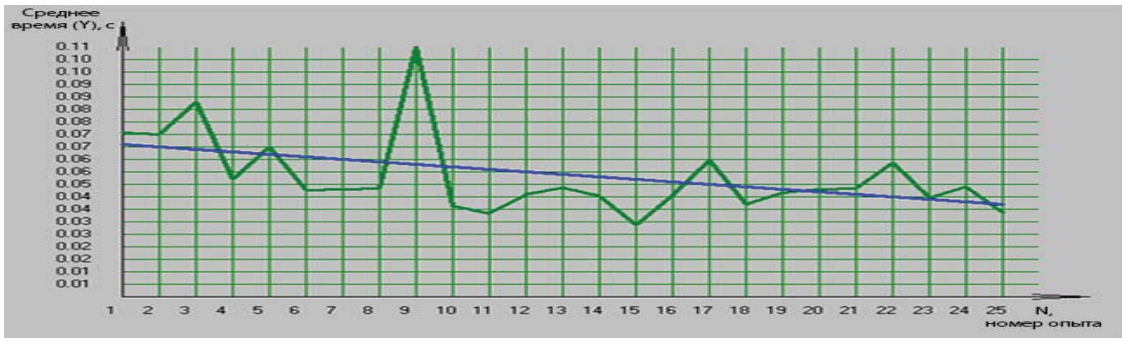


Рис. 7. Ввод цифр из множества {1, 2, 3} в окнах из множества {1, 2, 3,4}

$Y_{min} = 0.035$; $Y_{max} = 0.11$; $Y = 0.0725$; $T = t_1 + t_{2.1} + t_{2.2} + t_{2.3} + t_{3.1} + t_{3.2} + t_4$.

Примеры двух (из шести) видеограмм с результатами оценивания ППО, характеризующего уровень утомления человека-оператора в конце рабочего периода приведены на рис. 8 и 9.

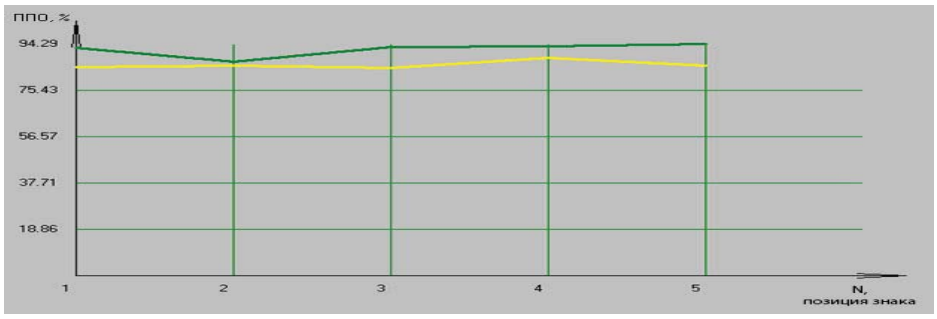


Рис. 8. Результат конечного замера по методике "Поиск сигнала в шуме"

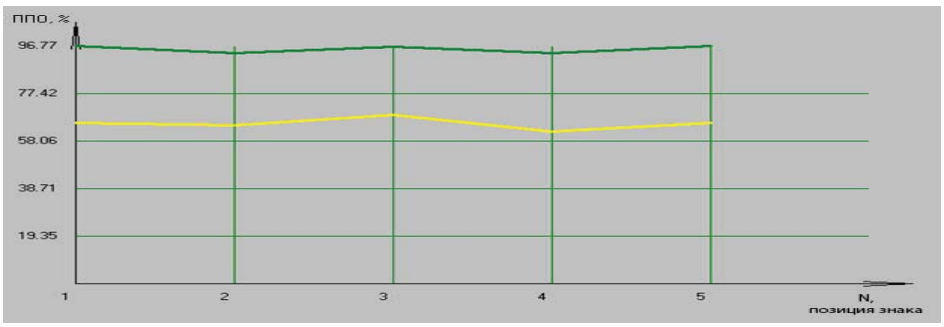


Рис. 9. Результат конечного замера по методике "Опознание"

Заключение.

Программное средство «Эффективность операторской деятельности в АИС», обеспечивающее оценку уровней работоспособности и утомления человека, контроль изменения значений соответствующих показателей в течение рабочего дня и выработку рекомендаций, следование которым позволяет снизить расход психических ресурсов, способствует повышению эффективности деятельности в условиях автоматизированных систем обработки информации и управления. Планируется расширение возможностей данного средства за счет введения в него моделей обработки человеком других форм представления данных/информации/знаний.

СПИСОК ЛИТЕРАТУРЫ

1. Понятие эффективности деятельности организации. URL: http://be5.biz/ekonomika/o003/45.html (Дата обращения – 27.04.2018)
2. Показатели эффективности деятельности организации: критерии и оценка. URL: https://www.kom-dir.ru/article/ 1457-pokazateli-effektivnosti-deyatelnosti (Дата обращения – 27.04.2018)
3. Петухов Г.Б. Основы теории эффективности целенаправленных процессов. М.: МО СССР, 1989. Ч. 1: Методология, методы, модели. 660 с.
4. Акофф Р., Эмери Ф. О целеустремленных системах / Пер. с англ. под ред. И.А. Ушакова. М.: Радио и связь, 1991. 272 с.
5. Каган М.С. Человеческая деятельность: опыт системного анализа. М.: Политиздат, 1974. 328 с.
6. Лукьянова Л.М. Системность решений по рыбохозяйственному комплексу // Рыбное хозяйство. 2014. №5. С. 57–64.
7. Лукьянова Л.М. Человекомашинное взаимодействие: Учебное пособие для бакалавриата по направлению подготовки «Информатика и вычислительная техника»: Инженерно-психологическое проектирование интерфейса взаимодействия в автоматизированных информационных системах. Калининград: ФГБОУ ВО «КГТУ», 2018. 80 с.
8. Организация взаимодействия человека с техническими средствами АСУ: Практическое пособие в 7 кн. / В.М.Гасов, Л. А. Соломонов; Под ред. В.Н. Четверикова. Кн. 7. Системное проектирование взаимодействия человека с техническими средствами. М.: Высш. шк., 1991. 142 с.
9. Котик М.А. Курс инженерной психологии: Учебник. 2-е изд., испр. и доп. Таллинн: Валгус, 1978. 364 с.
10. Мунипов В.М. Прикладная эргономика – эффективное средство рыночной экономики // Прикладная эргономика. № 1. 1993. С. 29–32.
11. Литвак И.И. Эргономические проблемы проектирования и эксплуатации средств отображения // Прикладная эргономика. № 1. 1993. С. 5–12 с.
12. Леонова А.Б. Психодиагностика функциональных состояний человека. М.: Изд-во МГУ им. М.В. Ломоносова, 1984. 200 с.

УДК 338.26

ОПЕРАТИВНАЯ АНАЛИТИЧЕСКАЯ ОБРАБОТКА ДАННЫХ МОНИТОРИНГА ОКУПАЕМОСТИ РЕАЛЬНЫХ ИНВЕСТИЦИЙ

Смирнова Елена Юрьевна
Санкт-Петербургское государственное унитарное предприятие
«Санкт-Петербургский информационно-аналитический центр»
Транспортный пер., 6, Санкт-Петербург, 191040, Россия
e-mail: elena.smirnova@iac.spb.ru

Аннотация. Технология оперативной аналитической обработки данных рассматривается в контексте стратегического бюджетирования для решения задачи формирования OLAP-куба показателей оценки эффективности капитальных вложений. Проблема оценки результативности инвестиционных проектов и соизмерения их эффективности на полном сроке окупаемости вложений в условиях роста макроэкономической неопределенности сохраняет актуальность. Критерии, по которым принимается решение об инвестировании на этапе планирования, в дальнейшем не всегда допускают сопоставление финансовых результатов для ведения аудита по завершении этапа реализации проекта. Предлагается в качестве метрики для оценки окупаемости вложений на этапе эксплуатации объекта инвестирования после прохождения денежным потоком точки безубыточности использовать текущий среднегодовой индекс рентабельности инвестиций. Такой подход допускает сопоставление разнородных (по объемам вложений и срокам реализации) инвестиционных проектов в составе долгосрочной программы и является методической основой для ведения предприятием экономического мониторинга окупаемости вложений на полном жизненном цикле проекта.

Ключевые слова: инвестиционный проект; капитальные вложения (CAPEX); индекс рентабельности; мониторинг; контроллинг; стратегическое бюджетирование; проектное управление; оперативная аналитическая обработка данных (OLAP); экономика обратной связи.

CAPITAL EXPENDITURES PROFITABILITY MONITORING DATA ONLINE ANALYTICAL PROCESSING

Smirnova Elena
St. Petersburg State Unitary Enterprise «St. Petersburg Information and Analytical Centre»
6 Transportnyj per., St. Petersburg 191040, Russia
e-mail: elena.smirnova@iac.spb.ru

Abstract. OLAP-technology is considered in the context of strategic budgeting for building a hypercube of CAPEX effectiveness indicators. The problem of investment projects efficiency assessment and commensurability of long-term effectiveness for the full payback period with increasing macroeconomic uncertainty still remains relevant. The criteria used to make investment decisions at the planning stage do not always allow further financial results comparison for post-completion audit. We suggest to use the current average annual profitability index as a metric to assess investment profitability after the actual breakeven point. Using such approach, we can compare heterogeneous – in amounts and terms – investment projects as part of a long-term program, and it can serve as a methodical basis for economic monitoring of investment profitability across the full life cycle of investment project.

Keywords: investment project; capital expenditures (CAPEX); profitability index; monitoring; controlling; strategic budgeting; project management; online analytical processing (OLAP); feedback economy.

Проблема регулярного измерения, корректного сопоставления и сводной оценки эффективности долгосрочных проектов в условиях роста глобальной макроэкономической неопределенности сохраняет свою актуальность. Насущной практической задачей для развивающихся российских предприятий является ведение детализированного регулярного мониторинга фактической окупаемости инвестиционных программ, которое возможно в рамках проектного подхода к управлению и на основе использования информационных технологий анализа данных.

Системный подход к проектному управлению капитальными вложениями принципиально опирается на деятельности субъекта обратной связи (контролера), наблюдающего за состоянием объекта инвестирования и на основе анализа отклонений, уточняющего плановые параметры или принимающего корректирующие решения для достижения запланированных результатов. Анализ экономической эффективности потока проектов в составе инвестиционной программы предприятия требует оценки текущего достигнутого уровня и динамики текущих показателей финансовой отдачи на стадии эксплуатации тех объектов, для создания которых инвестиции были реализованы. Необходимо построение рабочего процесса экономического мониторинга окупаемости инвестиционной программы, объединяющего процессы сбора, структурирования и обобщения информации на полном жизненном цикле реализованных проектов. При этом именно эксплуатационная стадия жизненного цикла созданных объектов в наибольшей степени характеризуется неопределенностью — как по длительности полезного функционирования объекта инвестирования, так и по волатильности элементов денежного потока.

Актуализация ключевых переменных, влияющих на промежуточные и конечные финансовые результаты, а также сводный уровень окупаемости вложений, должна проводиться регулярно, в автоматизированном режиме и с использованием единого централизованного набора данных. Эти требования приводят к необходимости ведения мониторинга на уровне автоматизированной информационной системы предприятия, реализующей обмен данными между подразделениями и поддерживающей решение долгосрочных задач стратегического управления. В современных условиях корпоративные информационные системы обычно включают в себя как транзакционные базы данных для ведения оперативного учета, так и многомерные аналитические хранилища, пригодные для автоматизации задач инвестиционного бюджетирования.

Непрерывный цикл управления эффективностью проектов в составе инвестиционной программы предприятия в процессе мониторинга реализуется по принципу внешней обратной связи (вторая петля в кибернетическом контуре с наблюдателем), представленной на рис.1.

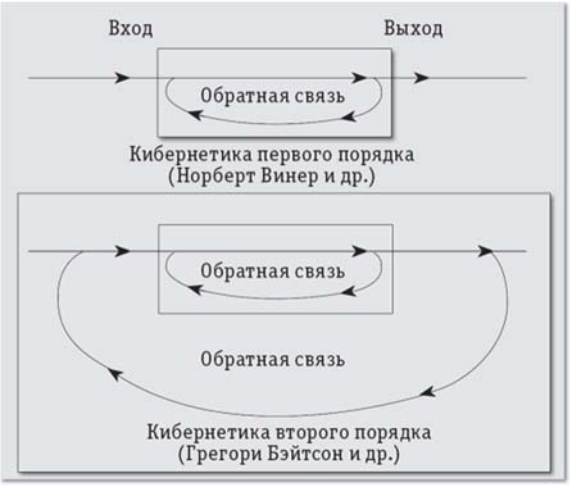


Рис.1. Схема обратной связи в кибернетическом контуре с наблюдателем [1]

В данном случае внутренняя система контура реализует учет информации о деятельности предприятия и затем финансовые данные, циркулирующие в автоматизированной системе учета, по мере их накопления и становятся полезной управляющей информацией стратегического характера, проходя неформальную аналитическую обработку на внешней петле с участием человека, интерпретирующего данные для принятия решений.

Применительно к решению задачи стратегического управления окупаемостью капитальных вложений данный кибернетический контур реализуется моделью инвестиционного контроллинга эффективности, основанная на «механизме рефлексивного мониторинга» [2], которая соответствует циклу управления НОРД/OODA (Наблюдение, Ориентация, Решение и Действие / Observe, Orient, Decide and Act), известному в теории системного анализа как «петля Бойда» [3]. Основными элементами аналитической модели инвестиционного контроллинга является архитектура формирования хранилища многомерной разделяемой информации на основе технологии OLAP (OnLine Analitical Processing) и непротиворечивая система критериальных показателей эффективности капитальных вложений.

Практический подход к организации рабочего процесса мониторинга требует ведения детализированный попроектный [4] учета текущих затрат и доходов на стадии эксплуатации созданных объектов. Однако в практике отечественного учета нередко планирование капитальных затрат ведется в составе расходной части бюджета [5], а фактические показатели результативности проектов не выделяются из потока сводных показателей предприятия для сравнения с плановой финансовой моделью.

Для ведения мониторинга окупаемости инвестиций необходим попроектный реестр объектов мониторинга. В составе полей записи данных по каждому проекту в реестре необходимо хранить не только исходную информацию, но и аналитические признаки для группирования (управленческие классификаторы), обозначающие сходство проектов (отрасль, технология, территория, окупаемость). Для подготовки текущей отчетности в схему реестра данных целесообразно также включить расчетные признаки группирования проектов по измерениям окупаемости: проект работает лучше (или хуже) утвержденного плана по выбранному критерию; пройдена ли точка инвестиционной безубыточности (самоокупаемость капитальных затрат). Собираемые из разных источников данные затем необходимо конвертировать в упорядоченную многомерную структуру (гиперкуб), допускающий оперативную аналитическую обработку. Примерная структура данных в реестре мониторинга окупаемости инвестиций представлена на рис.2.

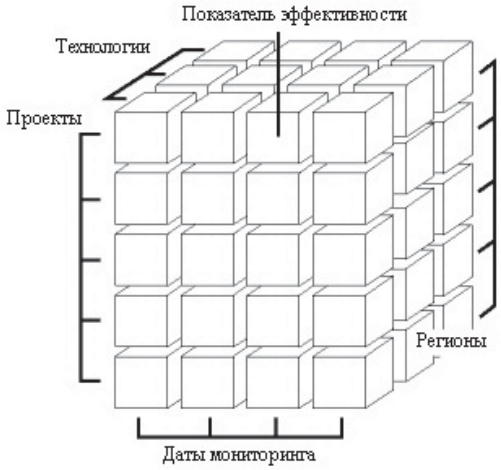


Рис.2. Структура OLAP- куба данных мониторинга окупаемости инвестиций

Регулярное пополнение истории данных мониторинга формирует информационно-статистическую базу для более достоверного обоснования новых вложений с учетом технологического, рыночного и финансового опыта реализованных ранее проектов: статистику отклонений от плана в ходе реализации, достигнутый уровень эффективности, модели действия внешних факторов риска и варианты корректирующих решений. Прогноз модели развития факторов, порождающих неблагоприятные отклонения в уровне эффективности проекта, дает возможность управления окупаемостью вложений, включая корректировку утвержденного плана и оценку вариантов прекращения реализации проекта, не приносящего плановой отдачи или вывода из эксплуатации объекта с отрицательной стоимостью владения.

С точки зрения практической реализации мониторинга окупаемости существует методическая трудность выбора критериев для оценки результатов в формате «план-факт» анализа. Традиционные критерии инвестиционного анализа, по которым принимается решение на этапе обоснования целесообразности проектов, не всегда допускают корректное сопоставление разнородных денежных потоков (как по объемам вложений, так и по срокам реализации). В данной статье предлагается авторский подход к формированию системы показателей эффективности, используемых как метрики в составе гиперкубов:

На этапе детализированного анализа проектов на дату мониторинга абсолютный эффект от реализации отдельного проекта предлагается измерять текущим частичным терминальным финансовым результатом (с учетом приведения элементов денежного потока вперед, к дате мониторинга).

На этапе сводной агрегированной оценки уровня окупаемости инвестиционной программы в целом предлагается использовать среднегодовой индекс рентабельности капитальных вложений (1+ «индекс скорости удельного прироста стоимости» [6]), средневзвешенный по терминальной стоимости первоначальных инвестиций проектов на дату мониторинга.

Таким образом, при условии ведения попроектного финансового учета затрат и результатов инвестиционной деятельности предприятия и использования автоматизированной технологии оперативной аналитической обработки данных (OLAP), для ведения мониторинга окупаемости инвестиционной программы предприятия можно использовать в качестве критерия эффективности среднегодовой индекс рентабельности вложений.

СПИСОК ЛИТЕРАТУРЫ

1. Черняк Л. Петля Бойда и кибернетика второго порядка // Открытые системы. СУБД. 2013. № 7. С. 54-56. URL: https://www.osp.ru/os/2013/07/13037357/ (дата обращения: 18.10.2018).
2. Бердников В.В. Проблемы формирования и перспективы применения аналитической модели контроллинга бизнеса // Экономический анализ: теория и практика. 2013. №46 (349). С.27-42.
3. Ивлев А.А. Основы теории Джона Бойда. URL: http://milresource.ru/Boyd.html (дата обращения: 18.10.2018).
4. Егоров Д.Е. Мониторинг инвестиционной деятельности: как отследить эффективность инвестиций с помощью системы бюджетного управления / Корпоративный менеджмент (сайт). URL: http://www.cfin.ru/finanalysis/invest/inv_monitoring.shtml (дата обращения: 18.10.2018).
5. Бариленко В.И. Методология мониторинга и аналитической оценки эффективности инновационных проектов на основе стейкхолдерского подхода. М., 2015. – 164 с.
6. Коган А.Б. Основной вопрос основных средств // Вестн. Новосиб. гос. ун-та. Серия: Социально-экономические науки. 2015. Т.15. Вып.1. С.102-109.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ

УДК 656.078.1

ЦИФРОВИЗАЦИЯ ПРОЦЕССОВ ВЗАМОДЕЙСТВИЯ СИСТЕМ АВИАЦИОННОГО ТРАНСПОРТНО-ЛОГИСТИЧЕСКОГО УЗЛА

Зайцев Евгений Николаевич, Коникова Елена Викторовна
Санкт-Петербургский государственный университет гражданской авиации
Пилотов ул., 38, Санкт-Петербург, 196210, Россия
e-mails: enzaitsev@mail.ru, elenavictorovnak@mail.ru

Аннотация. В статье рассматривается комплекс взаимодействия аэропорта, авиакомпании и УВД при приеме и обслуживании рейса. Описывается внедрение в аэропорту системы совместного принятия решений - Airport Collaborate Decision Making (A-CDM).

Ключевые слова: аэропорт; авиакомпания; взаимодействие; воздушное судно; наземное обслуживание рейса; авиационный транспортно-логистической узел; система совместного принятия решений в аэропорту.

DIGITAL FORM OF THE PROCESSES OF CO-OPERATION OF THE SYSTEMS OF AIR TRANSPORTATION LOGISTICS HUB

Zaitsev Evgeniy, Konikova Elena
Saint-Petersburg State University of Civil Aviation
38 Pilotov Str., St. Petersburg, 196210, Russia
e-mails: enzaitsev@mail.ru, elenavictorovnak@mail.ru

Abstract. In the article is examined the complex of co-operation of the systems of «Airport–Airline–ATC» at a reception and maintenance of the flight. Airport Collaborate Decision Making (A-CDM) - Airport system of joint acceptance of decisions introduction is described.

Keyword: airport; airline; interaction; aircraft; ground flight service; aviation transport-logistic junction; Airport-Collaborate Decision Making.

Определяющим показателем работы транспорта является транспортная составляющая цены перевозимого груза (пассажира) различными видами транспорта и зависит от их собственных проблем, а также от проблем при их взаимодействии.

Основными проблемами функционирования и развития авиационного комплекса, являются согласование и поддержание требуемых свойств при взаимодействии их техники, технологий, персонала, коммуникаций, энергообеспечения, экологии, безопасности, информационного, финансового и правового обеспечения.

Интеграция логистической деятельности требует слияния внутрипроизводственных и внешних логистических цепочек в единый интегральный Авиационный транспортно-логистический узел (как комплекс взаимодействия систем «Аэропорт-Авиакомпания-УВД»).

В процессе структурной перестройки на воздушном транспорте, на основе «принципов разделения авиационного предприятия на самостоятельное, выделение системы УВД в государственную службу ЕС ОрВД» с разделением объединенных авиационных предприятий на независимые хозяйствующие субъекты - авиационные предприятия и аэропорты с одновременной приватизацией и акционированием, происходит разрушение взаимосвязей между предприятиями и внутри их.

В связи с этим, рассмотрение проблемы эффективного взаимодействия аэропорта (АП), авиакомпании (АК) и Госкорпарации по организации воздушного движения (УВД- управление воздушным движением) при подготовке и выполнении перевозок как собственных, так и во взаимодействии с другими видами транспорта является актуальным и требует решения на следующих принципах [1]:

– системности, который означает структурирование и решение проблемы вертикальными связями;

– комплексности, где взаимодействие по горизонтали определяется связями сотрудничества, партнерства, используя такие свойства больших систем, как синергия и адаптивность;

– трехмерности рассмотрения систем, подсистем и их модулей при взаимодействии;

– декомпозиции, разложения системы на подсистемы, модули и их элементы;

– эффективного сотрудничества при взаимодействии систем «Аэропорт-Авиакомпания-УВД» с учетом принципов маркетинга (ресурсов), менеджмента, внешней и внутренней логистики;

– единого методологического подхода при исследовании процессов взаимодействия систем «Аэропорт-Авиакомпания-УВД»;

– формализации процесса формирования организационных структур управления;

– непрерывной опережающей (проактивной) профессиональной, экономической, правовой и управленческой подготовки личного состава.

Эффективность взаимодействия систем «Аэропорт-Авиакомпания-УВД» зависит от свойств их элементов, обеспечивающих функционирование и развитие.

Рассмотрим работу авиационного транспортно-логистического узла при взаимодействии систем «Аэропорт-Авиакомпания-УВД» (рис. 1) на этапах приема, обслуживании и отправки воздушного судна (ВС), которая состоит из четырех основных фаз авиационного производства: «Прилет-А», «Прилет-Б», «Вылет-В» и «Вылет-Г».

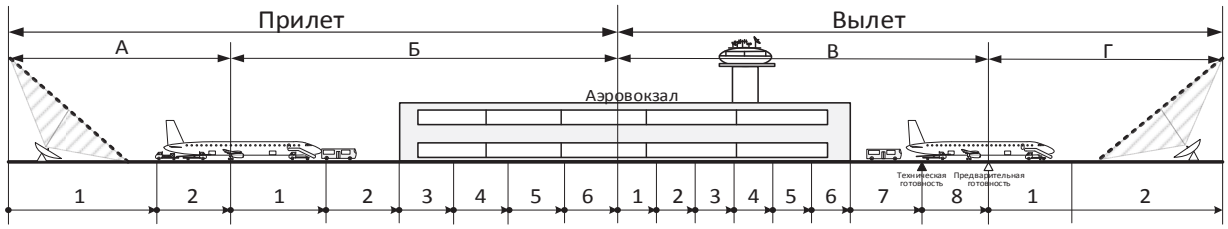


Рис. 1. Схема работы авиационного транспортно-логистического узла при приеме, обслуживании и отправки воздушного судна

Фаза «Прилет-А»: Движение ВС при приеме (посадке и рулении):

А1 – Взаимодействие аэропорта, авиакомпании и УВД при посадке ВС.

А2 – Руление и установка ВС на место стоянки.

Фаза «Прилет-Б»: Обслуживание прилетающих пассажиров:

Б1 – Высадка пассажиров из ВС.

Б2 – Доставка пассажиров к аэровокзалу.

Б3 – Пограничный контроль.

Б4 – Выдача багажа.

Б5 – Таможенный контроль.

Б6 – Выход прилетающих пассажиров из аэровокзала.

Фаза «Вылет-В»: Обслуживание вылетающих пассажиров:

В1 – Прибытие вылетающих пассажиров в аэровокзал.

В2 – Досмотр пассажиров и багажа на входе в аэровокзал.

В3 – Регистрация пассажиров и оформление багажа.

В4 – Таможенный контроль и пограничный контроль.

В5 – Предполетный досмотр.

В6 – Контроль явившихся пассажиров на посадку в ВС и посадка в транспортное средство (ТС), доставляющего к месту стоянки (МС) ВС.

В7 – Доставка пассажиров к МС ВС.

В8 – Посадка пассажиров в ВС.

Фаза «Вылет-Г»: Движение ВС по аэродрому при вылете:

Г1 – Выпуск, руление ВС с места стоянки к месту старта.

Г2 – Старт, разбег по взлетно-посадочной полосе (ВПП) и взлет ВС.

Г3 – набор высоты ВС.

В соответствии основными понятиями общей теории систем (система, элементы, связи, свойства, структура, функции, параметры и среда взаимодействия, характеризующие строение, функционирование и развитие систем), рассмотрим методологию формирования комплекса взаимодействия систем с использованием матричных моделей.

На рис. 2 представлен комплекс взаимодействия систем «Аэропорт-Авиакомпания-УВД» в соответствии с принципами системности, комплексности, трехмерности в виде трехмерной матрицы размера *I*x*N*x*J*:

Ось *I*- Элементы системы «Авиакомпания».

Ось *N* - Элементы системы «Аэропорт».

Ось *J* - Элементы системы «УВД».

Параметры (свойства) элементов систем «Аэропорт» и УВД, взаимодействующие при приеме, обслуживании и выпуск ВС должны соответствовать параметрам (свойствам) ВС.

1. Матрица размера $I \times N \times j$ при $i = \overline{1, I}$; $n = \overline{1, N}$; $j = 1$.

Матраца взаимодействия элементов систем АК и АП с *j-м* элементом системы УВД

2. Матрица размера *I* x *J* x *n* при $i = \overline{1, I}$; $n = 1$; $j = \overline{1, J}$.

Матрица взаимодействия систем АК и УВД на *n-ом* этапе работы АП

3. Матрица размера *N* x *J* x *i* при $i = 1$; $n = \overline{1, N}$; $j = \overline{1, J}$.

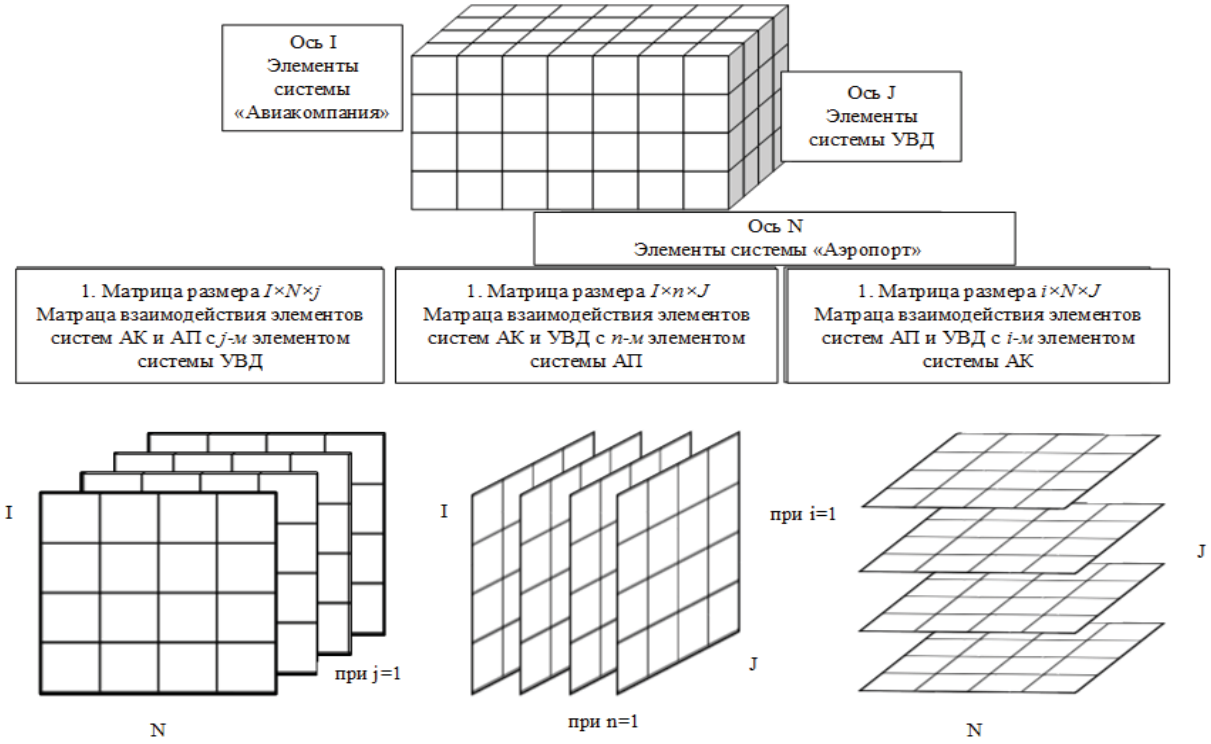


Рис. 2. Трехмерная структура комплекса взаимодействия систем «Авиакомпания-Аэропорт-УВД»

Матрица взаимодействия систем АП и УВД на *i-ом* этапе работы АК

Рассмотрение взаимодействия системы аэропортового комплекса «Аэропорт – Авиакомпания – УВД», на принципах трехмерной матрицы взаимодействия элементов авиационного транспортно-логистического узла, позволяет формировать модели, выявлять проблемные области, формировать системы поддержки принятия решений и оценивать деятельность транспортной системы.

Высокая эффективность комплекса взаимодействия систем «Авиакомпания-Аэропорт-УВД» может быть обеспечена путем создания единого цифрового пространства авиационного транспортно-логистического узла.

Под эгидой ИАТА, Ассоциации аэропортов ACI и Евроконтроля создана и постоянно актуализируется «Система совместного принятия решений в аэропорту» (Airport Collaborate Decision Making) [2,3,4,5]. A-CDM как проект был запущен в 2002 году по инициативе Экспериментального центра Евроконтроля. A-CDM применяется в 20 аэропортах Европы (Zurich, Frankfurt, Charles De Gaulle пр.).

A-CDM - (Airport-Collaborative Decision Making Portal) решение, созданное на облачной платформе, предназначено для усовершенствования управленческих процессов службами аэропортов.

Портал A-CDM объединяет всю внутреннюю систему аэропорта в одно целое и помогает правильно расставить рабочие приоритеты: своевременно разделять и доставлять определенную информацию до необходимого подразделения. Такой подход совершенствует наземное управление воздушным транспортом, стабилизирует расписание рейсов и улучшает обслуживание пассажиров.

Характеристики A-CDM:

– процесс совместного принятия решений (Collaborative Decision Making, CDM) позволяет всем его участникам участвовать в принятии затрагивающих их решений по организации воздушного движения (ОрВД);

– процесс CDM будет действовать по отношению к решениям всех уровней, начиная от долгосрочного планирования и кончая реальными операциями;

– процесс CDM можно применять как активно, так и пассивно, посредством совместно согласованных процедур;

– эффективное управление информацией и совместное ее использование позволят всем участникам процесса получать информацию, оказывающую важное влияние на решения других участников;

– любой участник процесса может предложить вариант решения (это приносит особую пользу в сочетании с эффективным осуществлением функции управления информацией).

Задачи системы A-CDM для аэропорта заключаются в повышении эффективности планирования и использования ресурсов, обеспечении бесперебойной работы аэропорта при тесном взаимодействии всех партнеров по A-CDM.

Ключевые концептуальные изменения включают следующие решения:

– процесс совместного принятия решений на стратегическом этапе обеспечит оптимизацию использования средств для получения максимальной отдачи и служит основой для прогнозируемого распределения и планирования;

– процесс коллективного принятия решений, по мере возможности, на предтактическом этапе позволит корректировать использование средств, распределение ресурсов, прогнозируемые траектории, структуризацию

воздушного пространства и планирование времени прибытия/отправления для аэродрома Шереметьево и района воздушного пространства в целях устранения любого дисбаланса;

– на тактическом этапе действия будут включать динамичное изменение времени прибытия/отправления для аэродрома и района воздушного пространства и корректировку расписания пользователями.

Аэропорт Шереметьево является первым аэропортом в России, который начал полноценную разработку и внедрение процедур A-CDM, используя при этом собственную разработку, не уступающую по своим возможностям и функциональности лучшим мировым аналогам. A-CDM в аэропорту Шереметьево создана на базе единой информационной платформы «Синхрон» [6].

Столкнувшись с ограничением технических возможностей, аэропорт Шереметьево принял решение по развитию инфраструктуры и инновационных технологий. Изучив зарубежный опыт, специалисты Шереметьево совместно с ОАО «Аэрофлот» и филиалом «МЦ АУВД» ФГУП «Госкорпорация по ОрВД» создали рабочую группу и разработали Концепцию внедрения системы совместного принятия решений A-CDM (Airport Collaborative Decision Making) в аэропорту Шереметьево.

В настоящее время в аэропорту Шереметьево полностью внедрен элемент A-CDM № 2 «Изменяемое время руления». Параллельно продолжаются разработки и внедрения этапов элементов A-CDM: № 0 «Система обмена информацией», № 1 «Поэтапный подход», № 3 «Общая последовательность действий при подготовке к отправлению» и № 4 «Система совместного принятия решений в неблагоприятных условиях».

Результат - рост пунктуальности отправления рейсов до 95,6% (1-ое место в Европе по данным FlightStatshttp://www.flightstats.com).

Задачи системы A-CDM для аэропорта Шереметьево заключаются в повышении эффективности планирования и использования ресурсов, обеспечении бесперебойной работы аэропорта при тесном взаимодействии всех партнеров по A-CDM.

Таким образом, целью внедрения стандарта A-CDM и его оптимизации является объединение экосистемы аэропорта (аэропортовые службы, авиакомпании, хендлинговых операторов и диспетчерские службы) для достижения эффективного и прозрачного взаимодействия и своевременного предоставления реальной информации. Это обеспечит лучшую организацию воздушного движения, позволит минимизировать задержки рейсов и увеличить пропускную способность аэропорта, предложить пассажирам более высокий уровень обслуживания за счет интегрированного подхода к организации.

В основе процесса A-CDM лежат принципы прозрачности и обмена информацией. Обмен информацией фактически является связующим звеном, объединяющим участников для достижения их общей цели - эффективной координации деятельности аэропорта, и фундаментом для других элементов концепции A-CDM. Обмен информацией в рамках A-CDM помогает каждому участнику принимать локальные решения и облегчает внедрение элементов A-CDM путем соединения систем обработки данных участников A-CDM и обеспечения единого общего набора данных о статусе полета, что служит основой обмена информацией между партнерами.

СПИСОК ЛИТЕРАТУРЫ

1. Зайцев Е.Н., Коникова Е.В., Тецлав И.А., Шайдуров И.Г. Комплекс взаимодействия систем «Аэропорт – Авиакомпания - УВД» в системе смешанных перевозок. Вестник Санкт-Петербургского университета гражданской авиации. Под ред. М.Ю. Смурова / С.-Петербург: СПбГУ ГА, 2016, с. 101-117.
2. The manual Airport CDM Implementation / Eurocontrol. – 2017, 363p.;
3. Airport CDM Functional Requirements Document / Eurocontrol – 2009, 48p.;
4. Manual on Collaborative Air Traffic Flow Management / ICAO, Doc9971 – 2014, 160p.;
5. Airport – Collaborative Decision Making: IATA Recomendarions / IATA – 2018, 20p.;
6. Никулин А.О., Попов А.А. Внедрение процедур A-CDM в аэропорту Шереметьево / Научный вестник МГТУ ГА № 211, 2015, с.68-79.

УДК 656.078.1

РАЗРАБОТКА И ПРИМЕНЕНИЕ ИМИТАЦИОННЫХ МОДЕЛЕЙ ПРИ УПРАВЛЕНИИ ПОТОКАМИ ПАССАЖИРОВ В АЭРОВОКЗАЛАХ

Зайцев Евгений Николаевич[1], Пашкевич Алексей Георгиевич[2], Тецлав Илья Александрович[1], Шайдуров Иван Георгиевич[1]

[1] Санкт-Петербургский государственный университет гражданской авиации
Пилотов ул., 38, Санкт-Петербург, 196210, Россия
[2] ООО «Институт развития транспортных систем»
Мясницкая ул., 24/7 стр. 3, Москва, 101000, Россия
e-mails: enzaitsev@mail.ru, pashkevich@irts.su, tetslavil@gmail.com, naviaga@mail.ru

Аннотация. В статье рассмотрена дискретно-событийная имитационная модель обслуживания пассажиров в аэропорту Пулково созданная в среде AnyLogic. Обоснована необходимость применения имитационного моделирования в процессе принятия решений (ППР) при перераспределении ресурсов на более загруженные участки в авиационном транспортно-логистическом узле.

Ключевые слова: имитационное моделирование; управление потоками; авиационный транспортно-логистической узел.

DEVELOPMENT AND APPLICATION OF IMITATION MODELS AT CONTROL OF FLOWS IN PASSENGERS TERMINALS

Zaitsev Evgeniy [1], Pashkevich Aleksey [2], Teclav Ilya [1], Shaydurov Ivan [1]
[1] Saint-Petersburg State University of Civil Aviation
38 Pilotov Str., St. Petersburg, 196210, Russia
[2] LLC «Institute Development of Transport Systems»
27/3 build 3 Myasnitskaya Str., Moscow, 141100, Russia
e-mails: enzaitsev@mail.ru, pashkevich@irts.su, tetslavil@gmail.com, naviaga@mail.ru

Abstract. The article considers discrete-event simulation model of passenger service at Pulkovo airport created in the AnyLogic environment. The necessity of application of simulation modeling in the decision-making process (DMP) is substantiated when resources are redistributed to more loaded areas in the aviation transport and logistics node.

Keywords: simulation modeling; flow management; aviation transport-logistics node.

Введение.

Развитие и совершенствование транспортной системы управления перевозками предусматривает решение следующих задач, отмеченных в Транспортной стратегии РФ на период до 2030 года [1]:

– развитие крупных транспортных узлов, логистических распределительных центров, обеспечение их единой технологической совместимости;

– создание единой системы и информационной среды технологического взаимодействия в транспортном узле;

– создание интеллектуальных транспортных систем с использованием глобальной навигационной системы для повышения качества и безопасности подготовки и выполнения перевозок.

Интеграция логистической деятельности требует слияния внешних и внутрипроизводственных логистических цепочек в единый авиационный транспортно-логистический узел как комплекс взаимодействия систем «Аэропорт-Авиакомпания-УВД») (рис. 1) на этапах приема, обслуживания и отправки ВС, включает четыре основные фазы авиационного производства: «Прилет-А», «Прилет-Б», «Вылет-В» и «Вылет-Г», в котором взаимодействуют:

– Система «Аэропорт»;
– Система «Авиакомпания;
– Система «УВД».

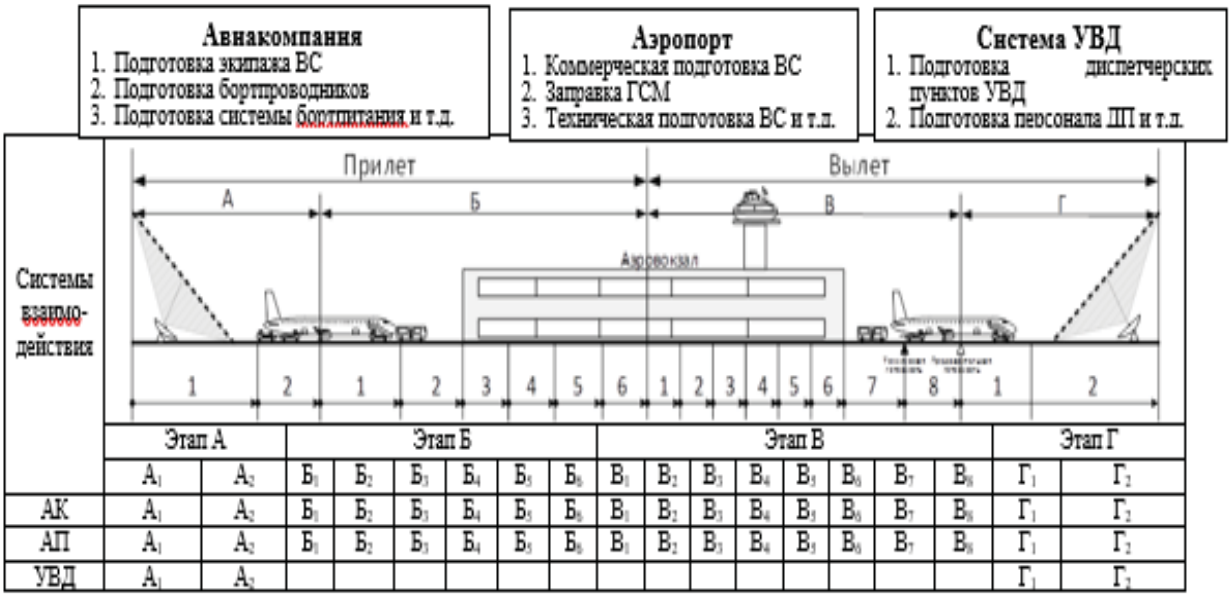


Рис. 1. Авиационный транспортно-логистический узел

В связи с этим, эффективность взаимодействия систем «Аэропорт-Авиакомпания-УВД» зависит от свойств их элементов, обеспечивающих подготовку, функционирование и развитие. Работу авиационного транспортно-логистического узла (АТЛУ).

Рассмотрим матричную структуру системы «Коммерческая подготовка ВС к рейсу» в АТЛУ (рис. 2), которая дает возможность комплексно рассматривать взаимодействие восьми элементов на всех этапах обслуживания вылетающих пассажиров из аэропорта.

Применяя матричную модель системы «Коммерческая подготовка ВС к рейсу» в АТЛУ [2,3], необходимо определить основные свойства элементов для формирования математической модели, оценки времени выполнения работ наземными службами аэропорта при обслуживании и подготовке рейсов, как в пункте вылета, так и в каждом пункте посадки.

	Элементы системы	Этапы системы подготовки пассажиров к рейсу							
		1. Прибытие в аэропорт	2. Досмотр на входе	3. Регистрация пассажиров и багажа	4. Таможенный и пограничный контроль	5. Предполетный досмотр	6. Учет пассажиров на посадке	7. Доставка к МС ВС	8. Посадка в ВС
		1	2	3	4	5	6	7	8
1	Пассажиры	1.1.	2.1.	3.1.	4.1.	5.1.	6.1.	7.1.	8.1.
2	Технологический процесс	1.2.	2.2.	3.2.	4.2.	5.2.	6.2.	7.2.	8.2
3	Персонал	1.3.	2.3	3.3.	4.3.	5.3	6.3.	7.3.	8.3
4	Техника	1.4.	2.4	3.4.	4.4.	5.4	6.4.	7.4.	8.4
5	Энергообеспечение	1.5.	2.5.	3.5	4.5.	5.5	6.5.	7.5.	8.5
6	Коммуникации	1.6.	2.6	3.6	4.6.	5.6	6.6.	7.6.	8.6
7	Экология	1.7.	2.7	3.7.	4.7.	5.7	6.7.	7.7.	8.7.
8	Безопасность	1.8.	2.8	3.8.	4.8.	5.8	6.8.	7.8.	8.8.

Рис. 2. Матричная структура системы «Коммерческая подготовка ВС к рейсу» в АТЛУ

Основные свойства пассажиров:
- $N_{пасс}$ – количество пассажиров;
- $N_{рк}$ – наличие ручной клади (нет багажа) и запрещенных предметов;
- KL – класс обслуживания пассажиров;
- VZ – возраст пассажиров;
- ZD – состояние здоровья (способность самостоятельно передвигаться);
- TP – тип пассажира (транзитный или трансферный).

Основные свойства персонала:
- $U_{перс.\ проф.}$ – уровень профессиональной подготовки (компетенций) персонала;
- $U_{перс.\ зд.}$ – необходимый уровень здоровья персонала;
- $U_{культ.}$ – уровень коммуникабельности персонала при обслуживании пассажиров.

Основные свойства оборудования:
- $N_{об}$ – количество оборудования;
- $P_{об}$ – производительность;
- $ЭР_{об}$ – эргономичность.

Основные свойства энергообеспечения при выполнении операции:
- $R_{ламп}$ – энергопотребление электросветотехнического обеспечения;
- $R_{об}$ – энергопотребление оборудования.

Основные свойства коммуникаций:
- $S_{комм}$ – площадь зон обслуживания.

Экспериментальные исследования в аэропорту Пулково (рис. 3) показали, что на этапах регистрации, досмотре, посадки образуются скопления пассажиров, которые блокируют проходы, что приводит к задержке пассажиров других рейсов и приходится отстранять их от рейса.

Ключевыми факторами образования очередей при обслуживании пассажиров в аэропорту являются материально-техническое обеспечение и расстановка ресурсов.

С развитием автоматизированных систем управления аэропортовым производством, разработанных на базе киберфизических систем в соответствии с принципами Индустрии 4.0 [4,5,6], совершенствуются процессы принятия решений с использованием имитационных моделей – цифровых двойников системы обслуживания пассажиров (рис. 4).

Главной особенностью цифрового двойника является возможность подключить его к физическому оригиналу путём передачи данных от множества установленных на нём датчиков и других «умных» устройств. В результате цифровой двойник функционирует параллельно с реальным объектом и может применяться, для диагностики, прогнозирования поведения объекта в сбойных ситуациях и комплексной оптимизации процесса обслуживания пассажиров.

Модель обслуживания пассажиров является инструментом, обеспечивающим количественные и качественные результаты вероятных последствий альтернативных решений (гипотез), сформулированных на стадии планирования («Что будет, если ...?»). Это вносит аналитический вклад в процессы планирования и принятия решений.

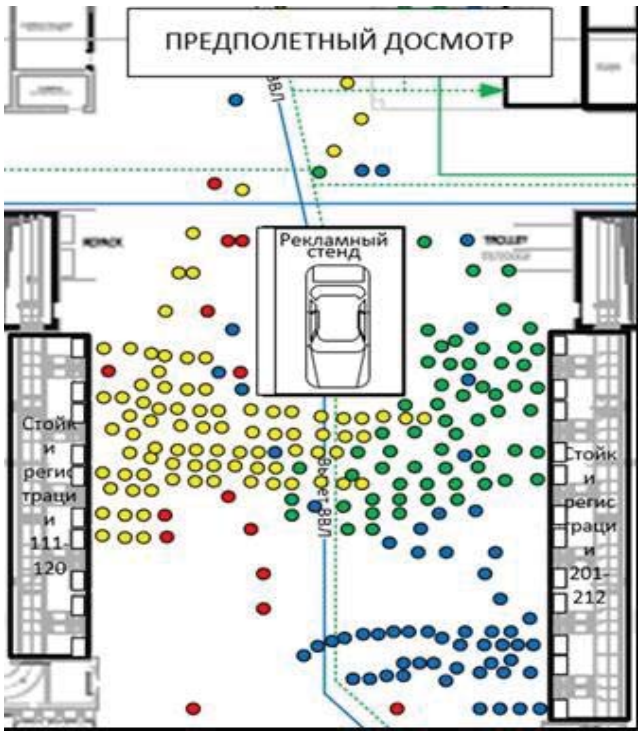


Рис. 3. Скопления пассажиров в зоне регистрации аэровокзала

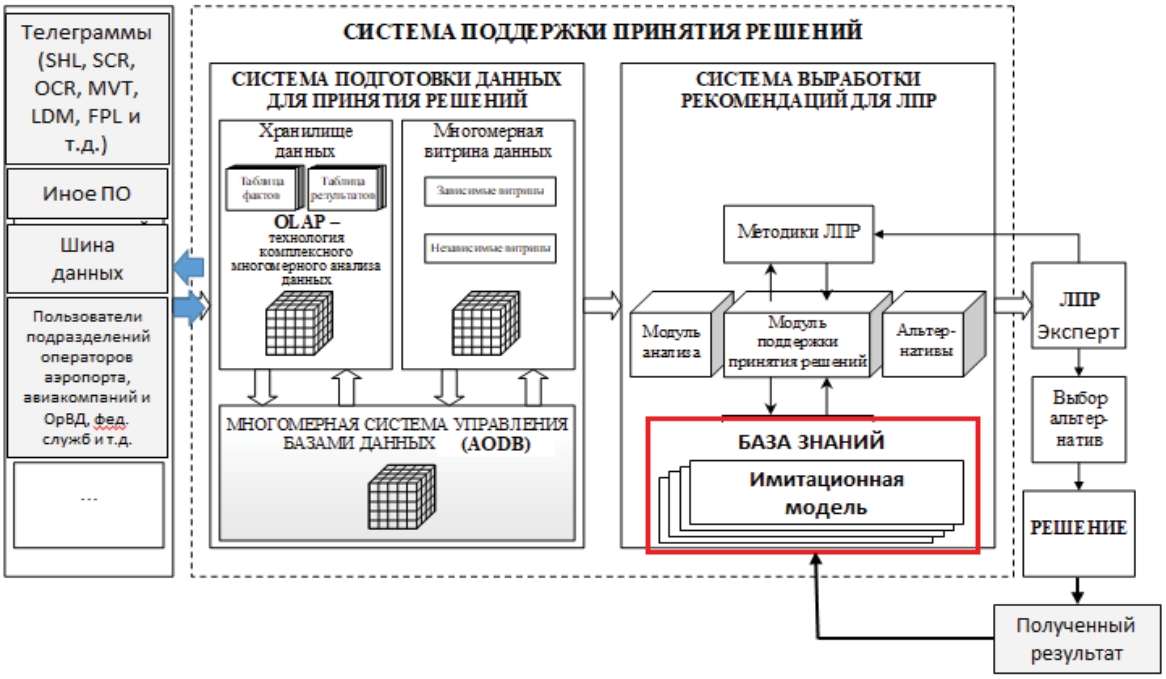


Рис. 4. Схема организации информационных потоков в системе поддержки принятия решений с самообучением

Модель может быть использована различными способами для обеспечения информацией участников этого процесса, в т. ч.:

– Понимание функций существующей инфраструктуры;

– Предоставление данных спроса для соответствующих вариантов анализа, проектирования и определения мощности (пропускной способности) объектов новой инфраструктуры и эксплуатационного (оперативного) обслуживания пассажиров;

– Понимание влияния изменения маршрутов, регулярности, скорости или доступности услуг в зонах общего пользования на пассажиров и доходы аэропортов.

Результаты модели предоставят количественную информацию, которая используется для разработки технологических схем обслуживания пассажиров, анализа рентабельности, финансового анализа и экологической оценки.

Модели обслуживания пассажиров включают в себя значительные объемы информации, которые описывают большое количество передвижений и обслуживания пассажиров в аэровокзале за определенный

период времени (например, какой-то конкретный час или день). Модели также содержат информацию о расписании прилетов и вылетов самолетов, планировочных схем площадей аэровокзала, свойств пассажиров и средств труда.

Модель позволяет определять загруженность технологических зон аэровокзала текущим пассажиропотоком или оценить потребностей в пропускной способности на долгосрочный период.

Для достижения требуемого функционала модели часто требуется сбор значительных (нередко трудоемких и дорогостоящих) исходных данных, полученных из стандартных статистических данных.

Этапы разработки модели

Перед проведением любых действий по моделированию необходимо в полном объеме понимать требования и функции этой модели. Это послужит гарантией того, что модель будет обеспечивать результат, который важен для проекта и обеспечивает ему качественную оценку. Этап определения задач моделирования рассматривает требуемый тип модели, уровень детализации исходных данных и способ проведения расчетов.

Далее следует этап сбора всех требуемых данных, необходимых также для этапов калибровки и проверки, и разработки модели. Целью этапа сбора данных является определение репрезентативной выборки статистических данных обслуживания пассажиров в аэровокзале за определенный период времени, а также факторы, способствующие возникновению сбойных и нештатных ситуаций и изменению условий обслуживания пассажиров.

Процесс калибровки и проверки направлен на обеспечение того, чтобы синтезированный набор соответствовал массиву данных наблюдаемого состояния обслуживания пассажиров. Это дает возможность изменить обслуживание пассажиров, услуги, спрос и математические алгоритмы таким образом, чтобы результаты моделирования лучше отражали существующее состояние обслуживания пассажиров. Этот этап дает возможность исправить любые ошибки при разработке модели, которые могут быть выявлены.

Далее разрабатываются модель обслуживания пассажиров, включающая сценарии сбойных и нештатных ситуаций при обслуживании пассажиров.

Имитационное моделирование позволяет в «безрисковой» виртуальной среде проводить эксперименты и определять оптимальные параметры для повышения эффективности объекта моделирования (рис. 5).

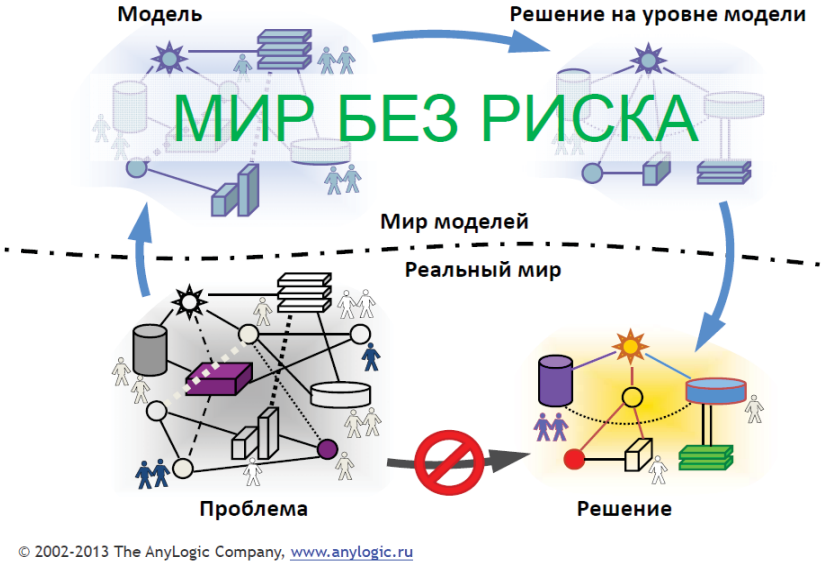


Рис. 5. Этапы процесса принятия решения в виртуальной «безрисковой» среде

Применение имитационной модели обслуживания пассажиров возможно при планировании ресурсов в долгосрочной, среднесрочной и краткосрочной перспективах, как в виде отдельного приложения, так и в составе системы управления ресурсами (RMS). Имитационная модель авиационного транспортно-логистического узла разработана в среде моделирования AnyLogic и может быть настроена для моделирования любой конфигурации аэропорта с помощью соответствующей настройки параметров.

Алгоритм формирования плана с использованием RMS и имитационной модели состоит из последовательных этапов (рис. 6).

Этапы формирования плана:

1. Формирование файла исходных данных из корпоративной базы данных;
2. При необходимости коррекция файла исходных данных ЛПР;
3. Формирование плана в RMS в файл;
4. Полученный файл используется как файл с исходными данными имитационной моделью необходимыми для проведения экспериментов;
5. Формирование в имитационной модели результатов проведения экспериментов в виде отчетов-рекомендаций для ЛПР.

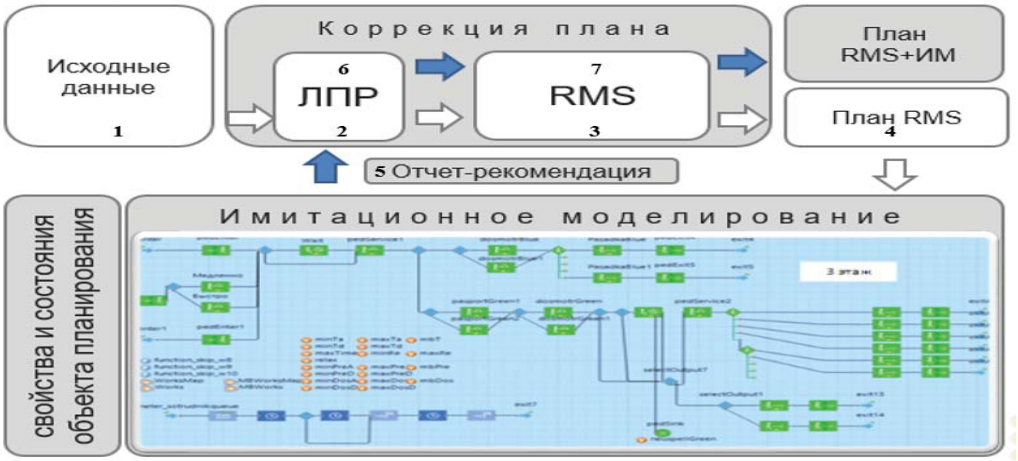


Рис. 6. Алгоритм формирования плана с использованием RMS и имитационной модели

Заключение.

Рассмотрена матричная структура и состояние системы подготовки пассажиров к вылету в авиационном транспортно-логистическом узле. Рассмотрен процесс принятия решения ЛПР при обслуживании пассажиров в аэропорту с использованием имитационной модели, разработанной в среде AnyLogic, с учетом динамично меняющейся обстановки.

Использование имитационного моделирования в проактивном управлении производственными процессами в аэропорту направлено на минимизацию потерь в сбойных ситуациях и повышение регулярности полетов ВС.

СПИСОК ЛИТЕРАТУРЫ

1. Транспортная стратегия РФ на период до 2030 г. (утверждена распоряжением Правительства РФ от 22 ноября 2008 г. № 1734-р)
2. Зайцев Е.Н., Коникова Е.В., Тецлав И.А., Шайдуров И.Г. Комплекс взаимодействия систем «Аэропорт – Авиакомпания - УВД» в системе смешанных перевозок. Вестник Санкт-Петербургского университета гражданской авиации. Под ред. М.Ю. Смурова / С.-Петербург: СПбГУ ГА, 2016, с. 101-117.
3. Коникова Е.В., Тецлав И.А. Разработка системы управления обслуживанием пассажиров в авиационном транспортно-логистическом узле с использованием имитационного моделирования. Транспорт России: проблемы и перспективы - 2017. Материалы Международной научно-практической конференции, 14-15 ноября 2017 г. СПб.: ИПТ РАН. – Санкт-Петербург. 2017. С. 395-399
4. Малыгин И.Г., Комашинский В.И., Аванесов М.Ю., Комиссаров С.А., Сорокин К.Н. Сети, информация и знания – основные драйверы четвертой индустриальной революции (Industrie 4.0) // Информация и Космос №1 / Радиотехника и связь. 2016. С. 14-25
5. Асаул А.Н., Малыгин И.Г., Комашинский В.И., Аванесов М.Ю. Концептуальные подходы к построению интеллектуальной мультимодальной транспортной системы РФ // Информация и Космос №3 / Радиотехника и связь. 2016. С. 8-17
6. Толуев Ю.И. Задачи имитационного моделирования при реализации концепции Индустрия 4.0 в сфере производства и логистики// Труды Восьмой всероссийской научно-практической конференции «Имитационное моделирование. Теория и практика» (ИММОД-2017) (г. Санкт-Петербург, 18-20 октября 2017 г.). СПб.: Изд-во ВВМ, 2017. С.57-65.
7. А.Э. Горев, В,Л. Швецов. Руководство по применению транспортных моделей в транспортном планировании и оценке проектов. — СПб.: ООО «Издательско-полиграфическая компания «КОСТА», 2016. — 128 с. (Серия «Библиотека транспортного инженера»).

УДК 656.078.1

ИСПОЛЬЗОВАНИЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ПЕРЕВОЗКЕ НЕГАБАРИТНЫХ ГРУЗОВ

Искандеров Юрий Марсович[1], Свистунова Александра Сергеевна[1], Чумак Александр Сергеевич[2]
[1] Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия В.О., 39, Санкт-Петербург, 199178, Россия
[2] ООО «НеваСпецТяж»
Московское шоссе, 25 корп.1, Санкт-Петербург, 196158, Россия
e-mails: iskanderov_y_m@mail.ru, svistunova_alexandra@bk.ru, chumak@nst-spb.ru

Аннотация. В статье рассмотрены преимущества использования интеллектуальной системы поддержки принятия решений при перевозке негабаритных грузов, учитывая существующие особенности такой перевозки. Показано, что ключевым элементом указанной системы является база знаний, содержащая релевантную информацию о перевозке. Дана характеристика технологии построения этой базы знаний, представлен фрагмент ее структуры и дано графическое изображение формального представления элемента базы знаний в виде семантического графа с оболочками.

Ключевые слова: интеллектуальная система поддержки принятия решений; негабаритный груз; перевозка; база знаний.

THE USE OF THE INTELLECTUAL DECISION SUPPORT SYSTEM FOR OVERSIZE CARGO TRANSPORTATION

Iskanderov Yury[1], Svistunova Alexandra[1], Chumak Alexander[2]
[1] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th liniya, Vasilievsky Island, St. Petersburg, 199178, Russia
[2] LLC «NevaSpecTyag»
25/1 Moscow highway, St. Petersburg, 196158, Russia
e-mails: iskanderov_y_m@mail.ru, svistunova_alexandra@bk.ru, chumak@nst-spb.ru

Abstract. The article presents the advantages of using an intelligent decision support system for the transportation of oversized cargo, taking into account the existing features of such transportation. It is shown that the key element of this system is a knowledge base containing relevant information on transportation. A characteristic of the technology for constructing this knowledge base is given, a fragment of its structure is presented and a graphic image of the formal representation of the knowledge base element in the form of a semantic graph with shells is given.

Keywords: intellectual decision support system; oversized cargo; transportation; knowledge base.

Введение.

В современных условиях критически важным фактором инновационного развития транспортной области становится разработка и внедрение интеллектуальных транспортных систем (ИТС), позволяющих качественно изменить процессы перемещения пассажиров и грузов [1,2]. Особенно важную роль играет использование ИТС при планировании, организации и проведении перевозки негабаритных грузов, поскольку указанные перевозки характеризуются уникальностью выполнения каждого проекта и высокой степенью риска его реализации.

В практической деятельности транспортно-логистических компаний часто возникает проблема перевозки крупногабаритных и тяжеловесных грузов, т.е. таких, требования к которым определены в пунктах 23.4 и 23.5 Правил дорожного движения РФ [3], а именно:

«23.4. Груз, выступающий за габариты транспортного средства спереди и сзади более чем на 1 м или сбоку более чем на 0,4 м от внешнего края габаритного огня, должен быть обозначен опознавательными знаками «Крупногабаритный груз», а в темное время суток и в условиях недостаточной видимости, кроме того, спереди — фонарем или световозвращателем белого цвета, сзади — фонарем или световозвращателем красного цвета.

23.5. Перевозка тяжеловесных и опасных грузов, движение транспортного средства, габаритные параметры которого с грузом или без него превышают по ширине 2,55 м (2,6 м — для рефрижераторов и изотермических кузовов), по высоте 4 м от поверхности проезжей части, по длине (включая один прицеп) 20 м, либо движение транспортного средства с грузом, выступающим за заднюю точку габарита транспортного средства более чем на 2 м, а также движение автопоездов с двумя и более прицепами осуществляются в соответствии со специальными правилами.»

Таким образом, нестандартный груз представляет собой громоздкий или тяжелый предмет, который из-за своей массы, размеров или специфических особенностей невозможно перевозить в закрытом дорожном транспортном средстве или закрытом контейнере, то транспортными средствами со стандартными характеристиками. Перемещение подобных грузов посредством железнодорожного или авиатранспорта - затруднительный и дорогостоящий процесс. Самым доступным на сегодняшний день и вместе с тем экономичным способом являются автомобильные перевозки грузов.

Перевозка негабаритных грузов - наиболее сложный вид перевозки, требующий специальной техники, наличия необходимых разрешений, предварительных согласований, при необходимости сопровождения и конвоя, специально обученных водителей, а также целого ряда других условий, соблюдение которых диктуется правилами перевозки негабаритных и сверхтяжелых грузов. Негабаритные и тяжеловесные грузы требуют системного подхода при транспортировке: детально разрабатывается маршрут, просчитываются наиболее выгодные, в том числе с экономической точки зрения, варианты перевозки. Перевозкой нестандартных грузов должны заниматься компании, располагающие парком специализированного транспорта и имеющие разрешение Минтранса России на ведение данного рода деятельности. Поскольку перевозка негабаритных грузов - сложный динамический процесс, для его осуществления необходим значительный объем достоверной разнородной информации. Очевидно, что в современных условиях для успешной реализации указанной транспортировки необходимо использовать релевантную систему поддержки принятия решений (СППР) [1,2]. Эта СППР дает возможность осуществлять планирование, управление и контроль всего процесса перевозки в режиме реального времени. Сведения, которые будут сформированы и использованы в СППР, а также информационный обмен в ходе перевозки имеют значительную коммерческую ценность, и представляют большой интерес для конкурентов и злоумышленников. Поэтому, учет аспектов обеспечения информационной безопасности в СППР также является актуальным и важным [4].

Для эффективного осуществления процесса транспортировки крупногабаритных и тяжеловесных грузов необходимо чтобы указанная СППР была интеллектуальной, т.е. представляла бы собой программно-техническую систему, построенную на основе методов инженерии знаний и позволяющую решать сложные задачи, связанные с переработкой информации на семантическом уровне [5]. Как известно, основным элементом такой интеллектуальной системы (ИС) является база знаний (БЗ), содержащая формализованные знания предметной области и обладающая следующими характерными свойствами [5]:

– пользователь не обязан обладать сведениями о структуре, представлении и манипулировании знаниями;
– обращение к БЗ осуществляется на языке, отражающем лишь семантические стороны запросов;
– отображение предметной области осуществляется с учетом пространственно-временных отношений;
– БЗ имеет механизмы, обеспечивающие индивидуальное развитие системы, т.е. имеет возможность пополнения знаний за счет привлечения новых знаний, а также на основе вывода уже имеемых в ней знаний;
– БЗ обеспечивает работу с противоречивыми, неполными и неточными знаниями.

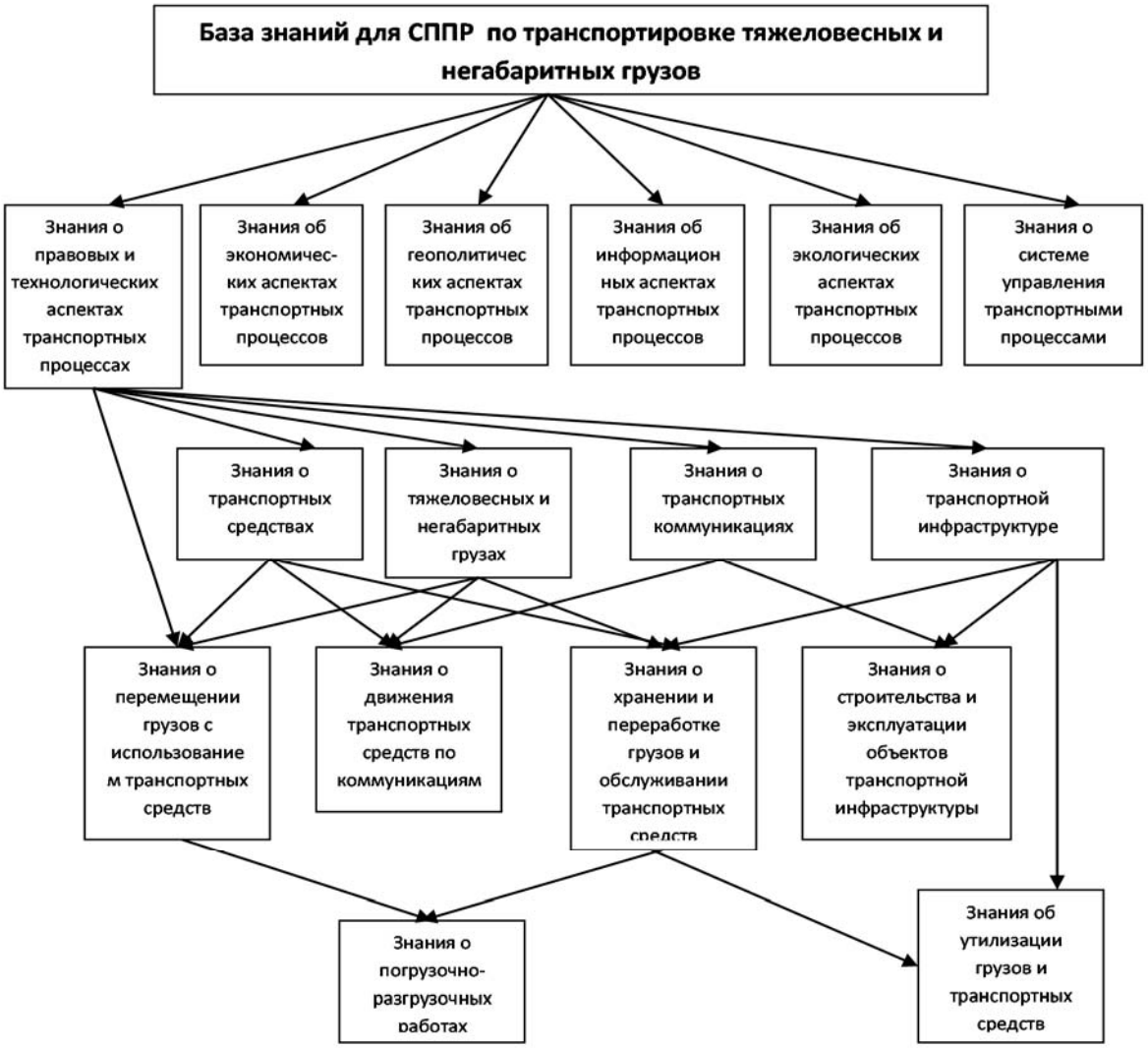


Рис.1. Фрагмент структуры БЗ для СППР по транспортировке тяжеловесных и негабаритных грузов

Знания о перевозках негабаритных грузов представляют собой факты, понятия, взаимосвязи, оценки, правила, эвристики, а также стратегии действий, накопленные в процессе получения, анализа и обобщения результатов практической деятельности, поскольку любая транспортировка негабарита является уникальной. В связи с этим заметим, что и никакого универсального тарифа на реализацию подобных услуг не существует. Перевозка негабаритных грузов планируется и осуществляется с учетом требований нормативных документов, регламентирующих такую перевозку. Например, в соответствии с Приказом Минтранса России [6], в тех случаях, когда ширина транспортного средства превышает пять метров или длина транспортного средства превышает 35 метров, или, когда на двухполосных дорогах при движении крупногабаритного транспортного средства ширина проезжей части для встречного движения составляет менее трех метров необходима разработка проекта организации дорожного движения по маршруту. Для того чтобы разработать такой проект в БЗ должны содержаться следующие сведения [6]:
– схема и описание маршрута движения;
– характеристики и параметры транспортных средств, участвующих в движении;
– схема (ы) размещения и крепления груза;
– график движения по маршруту с учетом интенсивности дорожного движения;

– схемы организации движения и прикрытия на участках, имеющих ограниченную видимость, и места, указанные в графе «Особые условия» специального разрешения, утвержденного Приказом Минтранса России [7], с указанием расположения автомобилей прикрытия, схемы изменения организации дорожного движения;

– порядок проезда наиболее сложных участков маршрута (поворотов, перекрестков, железнодорожных переездов, сужений проезжей части, участков с выездом на полосу встречного направления движения и с ограниченной видимостью) с нанесенной на схему траекторией движения;

– места осуществления контрольных промеров габаритов искусственных сооружений и коммуникаций в процессе перевозки;

– информация о необходимости полного или частичного перекрытия движения на участках дороги;

– места остановок и стоянок для отдыха и пропуска попутных (встречных) транспортных средств.

Более того, изложенные в проекте сведения должны подтверждаться видео- и фотоматериалами, отражающими реальное состояние объектов дорожной инфраструктуры. Ясно, что если проект выполняется в рамках временных и организационных ограничений, в условиях жесткой конкуренции, то БЗ будет эффективным инструментом для разработки указанного проекта, поскольку позволит минимизировать вероятность ошибок с учетом человеческого фактора. Создание БЗ является ключевым этапом формирования СППР для перевозки негабаритных грузов, поскольку качество БЗ напрямую влияет на эффективность функционирования СППР. Для создания БЗ для СППР используем технологию, разработанную в [5], но с учетом особенности организационных, технологических, психологических, инструментальных и других аспектов рассматриваемой предметной области. Указанная технология позволяет представить создание БЗ для СППР в виде системы типа “процесс”; на основе такого представления сформировать совокупность требований к БЗ; поставить и формализовать задачу создания БЗ в виде общей задачи принятия решений; применить в интересах построения БЗ двухэтапную модель и алгоритм поливариантного параллельного функционирования с согласованием решений в условных точках; выбрать релевантные методы, модели, алгоритмы и программные продукты выявления, извлечения, представления знаний, манипулирования ими, реализации и верификации БЗ [5].

На рис.1 представлен фрагмент структуры БЗ для СППР по транспортировке тяжеловесных и негабаритных грузов.

На рис.2 грузов дано графическое изображение формального представления элемента БЗ для СППР по транспортировке тяжеловесных и негабаритных в виде семантического графа с оболочками [5].

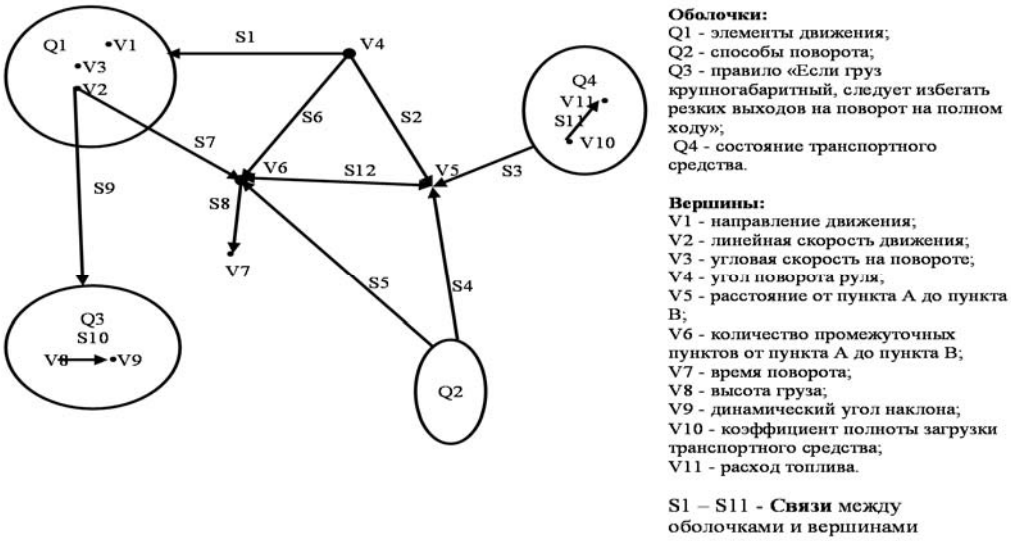


Рис. 2. Графическое изображение представления элемента БЗ для СППР по транспортировке тяжеловесных и негабаритных грузов в виде семантического графа с оболочками

Необходимо отметить, что оценка БЗ для СППР по транспортировке тяжеловесных и негабаритных грузов, выполненная с позиций двух основных групп критериев: качества работы и полезности, показала полное выполнение и системных, и пользовательских требований к БЗ.

Заключение.

Для создания БЗ для СППР транспортировки негабаритных грузов необходимо использовать технологию, разработанную в [5]. Использование этой технологии позволит:

– обеспечить обязательное получение требуемого конечного результата, т.е. соответствующей БЗ, оставляя при этом определенную свободу в выборе средств достижения этого результата;

– увязать воедино все аспекты (теоретические, организационные, психологические и др.) создания БЗ;

– обеспечить мониторинг хода разработки БЗ и управления им;

– реализовать эволюционный принцип «развивающегося ядра».

Создание и применение БЗ для СППР обеспечения процесса перевозки негабаритных грузов является важным направлением, имеющим значительные перспективы практического использования, особенно в процессе реализации концепции «Internet of Things» (IoT).

СПИСОК ЛИТЕРАТУРЫ

1. Искандеров Ю.М. Построение моделей интегрированной информационной системы транспортной логистики на основе мультиагентных технологий. Сборник статей Международной научно-практической конференции «Новая экономика и основные направления ее формирования». г.СПб, ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого», ISBN: 978-5-7422-5215-3, 2016г., с.62-69.
2. Искандеров Ю.М., Дорошенко В.И. Организация транспортно-технологических процессов на основе интегрированных информационных систем. Сборник статей Международной научно-практической конференции «Новая экономика и основные направления ее формирования». СПб., ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого», ISBN: 978-5-7422-5215-3, 2016г., с.53-62.
3. Правила дорожного движения РФ. Постановление Правительства РФ от 23.10.1993 N 1090 (ред. от 13.02.2018) «О Правилах дорожного движения» (вместе с «Основными положениями по допуску транспортных средств к эксплуатации и обязанности должностных лиц по обеспечению безопасности дорожного движения» (с изм. и доп., вступ. в силу с 18.03.2018).
4. Искандеров Ю.М., Чумак А.С. Обеспечение информационной безопасности процесса перевозки негабаритных грузов. Сборник X Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2017). СПб., 1-3 ноября 2017. СПОИСУ. – СПб., 2017г., с.276-277.
5. Искандеров Ю.М. Технология создания базы знаний для автоматизированной системы управления корпоративной сетью связи морского порта: диссертация ... доктора технических наук: 05.12.13. - Санкт-Петербург, 2005. - 243 с.: ил.
6. Приказ Министерства транспорта Российской Федерации от 15 января 2014 г. N 7 «Об утверждении Правил обеспечения безопасности перевозок пассажиров и грузов автомобильным транспортом и городским наземным электрическим транспортом».
7. Приказ Министерства транспорта Российской Федерации от 24 июля 2012 г. N 258 «Об утверждении Порядка выдачи специального разрешения на движение по автомобильным дорогам транспортного средства, осуществляющего перевозки тяжеловесных и (или) крупногабаритных грузов».

УДК 519

СИСТЕМА УПРАВЛЕНИЯ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ НА ОСНОВЕ НЕЙРОСЕТЕЙ: ЗАВИСИМОСТЬ РЕАЛИЗАЦИИ ОТ ТИПА РЕШАЕМЫХ ЗАДАЧ

Кудряшов Константин Витальевич, Балса Алдрин Раульевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: rus.256@yandex.ru, BalsaAR@gumrf.ru

Аннотация. Рассмотрены основные элементы системы управления беспилотным летательным аппаратом на основе нейросетей, а также задачи, решаемые с их помощью. Проанализированы варианты использования данных систем на различных типах летательных аппаратов.

Ключевые слова: беспилотный летательный аппарат; БПЛА; нейронная сеть; управление; автоматический.

CONTROL SYSTEM UNMANNED AERIAL VEHICLE ON THE BASIS OF NEURAL NETWORKS: THE DEPENDENCE OF THE IMPLEMENTATION ON THE TYPE OF TASKS

Kudryashov Konstantin, Balsa Aldrin
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya Str., St. Petersburg, 198035, Russia
e-mails: rus.256@yandex.ru, BalsaAR@gumrf.ru

Abstract. The main elements of the unmanned aerial vehicle control system based on neural networks and also the problems solved with their help are considered. The variants of using these systems on different types of aircraft are analyzed,

Keywords: unmanned aerial vehicle; UAV; neural network; control; automatic.

Введение.

Применение малогабаритных и легких беспилотных летательных аппаратов позволяет решать многие практические задачи, ранее не доступные широкому кругу пользователей. Беспилотные летательные аппараты находят применение в строительстве, геодезии, картографии, широко применяются при съемках фильмов и в скором времени будут повсеместно использоваться для курьерской доставки. Неисчерпаема возможность военного применения. Однако отсутствие пилота имеет серьезный недостаток: трудно осуществлять контроль за поведением летательного аппарата, особенно вне зоны прямой видимости. Частично эту проблему решает применение онлайн видео трансляции с камеры, расположенной на корпусе беспилотного летательного аппарата. Но такое решение затрудняет массовое коммерческое использование – каждому летательному аппарату потребуется оператор. К тому же возникают сложности в удаленных районах, без развитой системы мобильной связи. Автоматизированная система управления беспилотным летательным аппаратом, работающая без участия человека решает указанные проблемы, что указывает на актуальность данной темы.

Описание типов беспилотных летательных аппаратов. Существует огромное разнообразие типов летательных аппаратов [1,2]. Каждый тип предназначен и оптимизирован для выполнения конкретных практических задач. По принципу полета различают:

1) БПЛА с жестким крылом (БПЛА самолетного типа);
2) БПЛА с гибким крылом;
3) БПЛА с вращающимся крылом (БПЛА вертолетного типа);
4) БПЛА с машущим крылом;
5) БПЛА аэростатического типа.

Кроме БПЛА перечисленных пяти групп существуют также различные гибридные подклассы аппаратов, которые по их принципу полета трудно однозначно отнести к какой-либо из перечисленных групп. Особенно много таких БПЛА, которые совмещают качества аппаратов самолетного и вертолетного типов.

БПЛА самолетного типа [3]**.** Этот тип аппаратов известен также как БПЛА с жестким крылом. Подъемная сила данных аппаратов создается аэродинамическим способом за счет напора воздуха, набегающего на неподвижное крыло. Аппараты данного типа способны выполнять полеты на относительно большой высоте и большой скоростью. Длительность полета также высока. Существует большое разнообразие подтипов БПЛА самолетного типа, различающихся по форме крыла и фюзеляжа. Практически все схемы компоновки самолета и типы фюзеляжей, которые встречаются в пилотируемой авиации, применимы и в беспилотной.

БПЛА с гибким крылом**.** Это дешевые и экономичные летательные аппараты аэродинамического типа, в которых в качестве несущего крыла используется не жесткая, а гибкая (мягкая) конструкция, выполненная из ткани, эластичного полимерного материала или упругого композитного материала, обладающего свойством обратимой деформации. К БПЛА данного типа относят беспилотные моторизованные парапланы, дельтапланы и БПЛА с упруго деформируемым крылом. Беспилотный моторизованный параплан – аппарат на основе управляемого парашюта-крыла, снабжённый мототележкой с воздушным винтом для автономного разбега и самостоятельного полёта. Крыло, как правило, имеет форму эллипса или прямоугольника, оно может быть мягким, иметь жесткий или надувной каркас. Недостатком беспилотных моторизованных парапланов является трудность управления ими, так как органы управления не имеют жесткой связи с крылом. Также применение аппаратов данного типа затрудняют сложные погодные условия.

БПЛА вертолетного типа**.** Этот тип аппаратов известен также как БПЛА с вращающимся крылом. У аппаратов данного типа подъемная сила возникает на крыле (винте) во время его вращения в горизонтальной плоскости. Преимуществами БПЛА вертолетного типа являются способность зависания в точке и высокая маневренность. Однако существенным недостатком является низкая энергетическая эффективность данных аппаратов, что в свою очередь ограничивает массу полезной нагрузки.

БПЛА с машущим крылом**.** БПЛА с машущим крылом основаны на бионическом принципе – копировании движений, создаваемых в полете летающими живыми объектами – птицами и насекомыми. На данный момент серийно не производятся летательные аппараты данного класса, однако исследовательские работы в этом направлении ведутся по всему миру. Главные преимущества подобных летательных аппаратов, в теории, заключаются в очень высокой энергоэффективности и маневренности. Аппараты, основанные на имитации движений птиц, получили название орнитоптеров, а аппараты, в которых копируются движения летающих насекомых – энтомоптерами.

Принцип полета летательного аппарата определяет основные конструктивные решения, в том числе способы удержания аппарата в воздухе и маневрирования, что в свою очередь определяет алгоритм управления летательным аппаратом. Таким образом, для каждого типа БПЛА необходимо создавать уникальную систему управления, учитывающую его конструктивные особенности и сферу применения.

Система управления беспилотным летательным аппаратом непосредственно оказывает управляющие воздействия на органы управления летательным аппаратом, заставляя его менять свое положение в пространстве [3]. Решения на выдачу управляющих воздействий система принимает исходя из следующих входных параметров:

- Текущее положение летательного аппарата в пространстве;
- Цели полетного задания;
- Команды оператора с пульта дистанционного управления.

Система должна обеспечивать выполнение полетного задания, состоящего, в простейшем случае, из облета контрольных точек. Однако должна быть предусмотрена возможность ручного управления летательным аппаратом. К тому же любые маневры не должны приводить к потере управляемости летательного аппарата и выходу его в аварийные режимы полета, такие как сваливание, штопор и прочие. Таким образом, система управления беспилотным летательным аппаратом должна обеспечивать:

- Устойчивое и безопасное поведение летательного аппарата в воздухе;
- Выполнение управляемого полета, согласно полетному заданию или командам оператора.

Система управления беспилотным летательным аппаратом состоит из двух групп элементов: управляющая часть и исполняющая часть (рис. 1). Управляющая и исполняющая части связаны между собой радиоканалом.

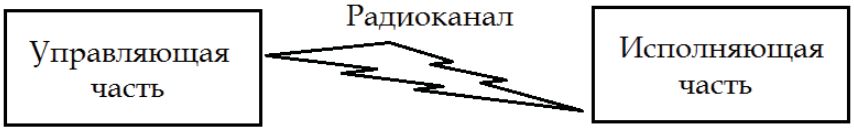


Рис. 1. Обобщенная схема системы управления беспилотным летательным

Управляющая часть предназначена для считывания команд оператора с органов управления, формирования команд управления и передачи команд на борт летательного аппарата в исполняющую часть. В состав управляющей части входят (рис. 2):

- Пульт дистанционного управления;
- Микроконтроллер с необходимой электрической схемой;
- Радио модуль;
- Аккумуляторная батарея.

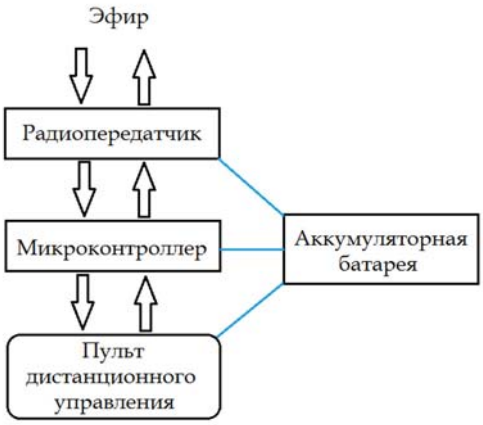


Рис. 2. Состав управляющей части

Пульт дистанционного управления содержит кнопки управления, переключатели и ползунки, а также может содержать жидкокристаллический дисплей, для отображения информации о различных параметрах. При помощи пульта осуществляется взаимодействие пользователя с системой.

Микроконтроллер содержит программу, которая считывает информацию с пульта дистанционного управления, формирует команды управления для летательного аппарата и отправляет их на радиопередатчик. Также микроконтроллер управляет отображением информации на дисплее. Микроконтроллер должен иметь достаточное для подключения всех органов управления число выводов, иметь достаточные объемы памяти, высокий уровень быстродействия.

Радио модуль транслирует команду управления в эфир. Радиопередатчик управляющей части и радиоприемник исполняющей части должны быть совместимы и иметь достаточную мощность, для обеспечения канала управления на требуемой дистанции.

Аккумуляторная батарея служит для автономного питания управляющей части. Батарея должна иметь необходимое для работы оборудование напряжение. Емкость батареи должна обеспечивать беспрерывную работу управляющей части в течении требуемого времени.

Исполняющая часть принимает по радиоканалу команды управления от управляющей части. На основе этих команд и информации, полученной от собственных датчиков, исполняющая часть принимает решения о поведении летательного аппарата в пространстве путем воздействия на органы управления летательного аппарата.

В состав исполняющей части входят (рис. 3):

- Радио модуль (позиция 1);
- Микроконтроллер с необходимой электрической схемой (позиция 2);
- Датчики положения в пространстве (позиция 3);
- Сервоприводы органов управления летательным аппаратом (позиция 4);
- Аккумуляторная батарея (позиция 5).

Радио модуль принимает команды от управляющей части по радиоканалу и передает их микроконтроллеру.

Микроконтроллер исполняющей части является центральным звеном всей системы управления беспилотным летательным аппаратом с использованием нейронных сетей. Он получает команды от управляющей части через радио модуль, считывает показания датчиков положения в пространстве.

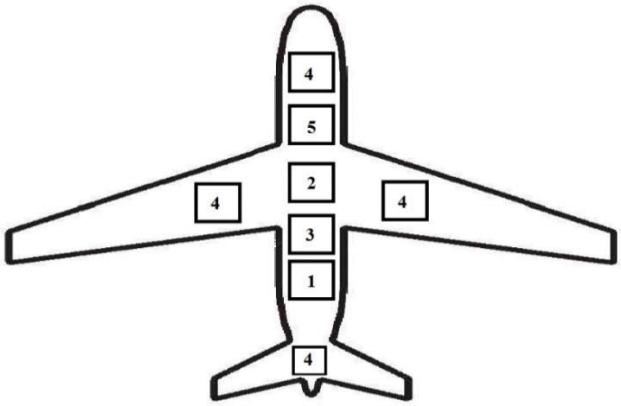


Рис. 3. Схема размещения исполняющей части на борту летательного аппарата

Специальный алгоритм на основе нейросетей производит анализ всей доступной информации и принимает решения на изменение параметров полета летательного аппарата в соответствии с текущей ситуацией. Принятые поправки в параметры полета передаются в сервоприводы органов управления летательным аппаратом. Микроконтроллер должен быть достаточно мощным, чтобы обеспечить необходимую скорость обработки сигналов и работы нейросети.

Датчики положения в пространстве передают в микроконтроллер информацию о положении летательного аппарата в пространстве. К таким данным относятся данные о текущих координатах с GPS датчика, углы наклона аппарата по осям координат и ускорение с акселерометра и гироскопа.

Сервоприводы органов управления летательным аппаратом преобразуют управляющие сигналы микроконтроллера в механические движения, которые отклоняют органы управления летательным аппаратом на необходимый угол и управляют подачей топлива двигателя летательного аппарата.

Аккумуляторная батарея служит для автономного питания всех элементов управляемой части и устройств летательного аппарата. Батарея должна иметь необходимое для работы оборудование напряжение. Емкость батареи должна обеспечивать беспрерывную работу всех элементов системы на все время полета.

Заключение.

При проектировании алгоритма управления БПЛА на основе нейросетей требуется учитывать:

- Тип летательного аппарата;
- Географию применения и погодные условия;
- Задачи, возлагаемые на БПЛА;
- Пределы автономности.

СПИСОК ЛИТЕРАТУРЫ

1. Беспилотные летательные аппараты в МЧС: виды и классификация [Электронный ресурс] / Пожарная безопасность: сайт пожарных и спасателей. Режим доступа: https://fireman.club/statyi-polzovateley/bespilotnyie-letatelnyie-apparatyi-v-mchs-rossii-vidyi-i-klassifikatsiya/, свободный. – Загл. с экрана.
2. Фетисов В.А. Беспилотная авиация: терминология, классификация, современное состояние. Уфа: ФОТОН, 2014.
3. Беспилотный летательный аппарат [Электронный ресурс] / Большая российская библиотека. Режим доступа: https://bigenc.ru/technology_and_technique/text/4087725, свободный. – Загл. с экрана.
4. Система управления полётом самолёта [Электронный ресурс] / Режим доступа: https://ru.wikipedia.org/wiki/Система_управления_полётом_самолёта, свободный. – Загл. с экрана.

УДК 658.5:004.94

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ СИСТЕМ СКЛАДИРОВАНИЯ КОНТЕЙНЕРНЫХ ТЕРМИНАЛОВ

Николаевский Николай Николаевич[1], Козлова Дарья Викторовна[2]
[1] Национальный исследовательский университет «Высшая школа экономики»
Кантемировская ул., 3, Санкт-Петербург, 194100, Россия
[2] Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: triplenick@mail.ru, dashakozlova1994@yandex.ru

Аннотация. В работе рассматриваются альтернативные варианты организации складских систем контейнерных терминалов. Проведен обзор литературы по соответствующей тематике, по результатам которого делается вывод об ограниченности проработки вопросов внедрения и эксплуатации складской системы контейнерного терминала с использованием стеллажей. Для оценки диапазонов характеристик грузопотоков, определяющих выбор наиболее предпочтительной схемы организации складской системы, разработана имитационная модель терминала. На базе разработанной модели реализованы эксперименты варьирования параметров, что позволило сформулировать рекомендации по использованию стеллажного способа хранения контейнеров.

Ключевые слова. контейнерный терминал; система складирования; имитационное моделирование; подъемно-транспортное оборудование.

SIMULATION OF CONTAINER TERMINAL STORAGE SYSTEM

Nikolaevskiy Nikolay[1], Kozlova Daria[2]
[1] National Research University Higher School of Economics
3 Kantemirovskaya St, St. Petersburg, 194100, Russia
[2] Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya Str., St. Petersburg, 195251, Russia
e-mails: triplenick@mail.ru, dashakozlova1994@yandex.ru

Abstract. The paper looks into the issues of alternative options of the container terminal storage system functioning. A preliminary literature overview in the respective area has shown that most of the studies consider the questions of staking storage system organization. At the same time there is a lack of methodological developments in the area of implementation of rack storage systems. The simulation model of storage of freights in a warehouse have been developed and realized. On the basis of the created model the experiment of variation of parameters was made. The results allowed to estimate the range of incoming and outgoing flow intensity, which determines preference of choosing storage system.

Keywords. container terminal; storage system; simulation modelling; material-handling equipment.

Введение.

Экономический рост и развитие уровня глобального товарообмена неотъемлемо сопровождается увеличением объемов транспортировки, в том числе с использованием контейнерных перевозок. В свою очередь, в условиях масштабной контейнеризации особую важность приобретают вопросы проектирования, исследования и модернизации контейнерных терминалов в части развития сервиса по обработке грузов для обеспечения соответствующих конкурентных преимуществ. При этом нельзя не отметить современные тенденции к массовой цифровизации логистических процессов, обусловленных интенсивным развитием и повсеместным внедрением информационных технологий, что определяет необходимость стремления к автоматизации процессов функционирования терминалов.

Контейнерный терминал – территория, на которой расположен комплекс технических средств и сооружений для выполнения операций, связанных с контейнерными перевозками. К этим операциям относятся прибытие и отправка, погрузка и выгрузка, сортировка и временное хранение контейнеров, а также их коммерческое и техническое обслуживание. Важнейшим технологическим элементом контейнерного терминала как логистической системы является складская зона для хранения контейнеров. Функционирование складской зоны предполагает обслуживание входящих и исходящих грузовых потоков посредством определенной технологии перегрузочных работ, характеризующейся структурой парка подъемно-транспортного оборудования (ПТО) и особенностями объемно-планировочного решения, которые в свою очередь и определяют пропускную способность технологического элемента [1].

В большинстве технологических систем хранения складирование контейнеров предполагает помещение их в штабель, друг на друга. Важно отметить, что такой способ имеет ряд недостатков. В первую очередь, существенным недостатком штабельного хранения является ограниченность высоты подъема и грузоподъёмности штабелируемой техники. Данное обстоятельство позволяет формировать штабель лишь в 5-6 ярусов для хранения порожних контейнеров и максимум в 4 яруса для груженных. При этом использование штабельной системы хранения затрудняет доступ к контейнерам, находящимся в глубине штабеля, что сильно ограничивает возможности к автоматизации перегрузочных процессов. Существенные ограничения приводят к увеличению площадей складской зоны и замедлению процесса обслуживания прибывающих и убывающих грузов. В связи с этим, в последнее время все чаще внимание стало уделяться альтернативным способам организации процесса складирования с использованием стеллажных конструкций. Такая система хранения должна обеспечивать лучшее использование объема склада в виду отсутствия ограничений по высоте, а строгое позиционирование грузовых единиц создает условия для полной автоматизации процесса.

Таким образом, в случае значительного роста грузооборота компании возникают дополнительные требования к увеличению пропускной способности, ускоряется оборачиваемость грузовых единиц, что, в свою очередь, ведет к увеличению количества порожних и груженых контейнеров, а как следствие к необходимости увеличения складских площадей. Однако расширение территории терминала далеко не всегда доступная опция,

поэтому возможным решением может являться модернизация, заключающаяся в отказе от штабельного хранения контейнеров и применения технологии стеллажного хранения грузовых единиц.

На начальном этапе исследования был проведен анализ научных источников по соответствующей тематике [3, 4, 5, 6, 7], по результатам которого были рассмотрены различные варианты организации складской зоны контейнерных терминалов с использованием стеллажного хранения. Отмечается, что размещение контейнеров в стеллажах обладает преимуществами обеспечения высокой плотности хранения, высокой пропускной способности и беспрепятственного доступа к целевому контейнеру без операций повторной обработки. Применение такой системы хранения должно позволить компаниям значительно экономить земельные площади на терминале, что благоприятно сказывается на финансовом положении предприятия (значительно снижаются затраты на аренду или содержание имеющихся территорий). Увеличения емкости склада можно добиться за счет увеличения количества ярусов хранения. Важно отметить, что системы складирования контейнеров с использованием стеллажей требуют создания принципиально новой инфраструктуры, определяемой особенностями структуры парка специализированного ПТО. Последнее обстоятельство обуславливает необходимость оценки экономической целесообразности внедрения новой технологии в виду значительных капитальных затрат.

Однако по результатам обзора отмечается недостаточность проработки конкретных рекомендаций по выбору наиболее предпочтительной из альтернативных схем организации складской зоны контейнерного терминала, поэтому было предложено оценить диапазоны характеристик входящих и выходящих грузопотоков, определяющих приоритетность использования конкретной схемы реализации технологического процесса.

Для решения указанной задачи на базе принципов теории массового обслуживания была разработана имитационная модель функционирования складской системы контейнерного терминала в части приемки и отправки грузов. Для создания модели использовалась программная среда AnyLogic в соответствии с дискретно-событийной парадигмой моделирования, что обеспечило использование элементов теории массового обслуживания, реализованных в виртуальной временной среде. При этом складская зона выступает в роли канала обслуживания входного и выходного потоков заявок. Для упрощения самой модели и оценки полученных результатов было принято решение все заявки-контейнеры заменить соответствующим эквивалентом контейнера – TEU. Такой подход позволит оценить показатели средней длины очереди и времени ожидания обслуживания при различных значениях интенсивностей входящих и выходящих потоков.

Реализация имитационной модели. В рамках данной работы ставится цель сравнительного анализа систем складирования при использовании штабельного и стеллажного способов хранения контейнеров посредством реализации имитационной модели процессов функционирования терминала. Важно отметить, что имитационное моделирование является современным средством решения задач и предполагает реализацию логики функционирования моделируемого объекта в виртуальной временной среде. При этом обеспечиваются возможности учета стохастических параметров и реализации различных экспериментов, что благоприятно сказывается на качестве получаемых результатов. Для достижения цели работы было принято решение разработать имитационную модель действующего контейнерного терминала компании ООО «Модуль», схема которого представлена на рис. 1, где под номером 1 обозначена открытая складская площадка для генеральных грузов, затаривания и разгрузки контейнеров, под номером 2 обозначен крытый склад, под номером 3 обозначены автомобильные пункты пропуска [2].

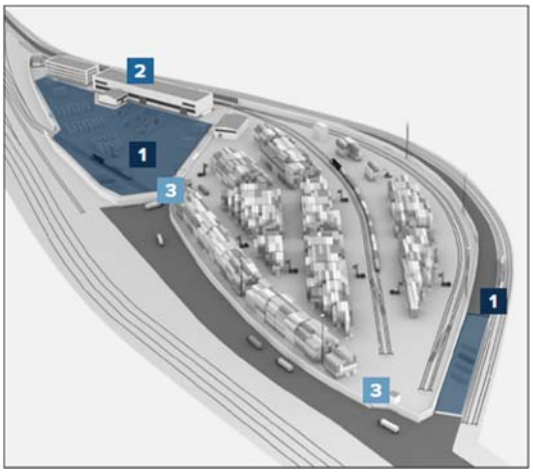


Рис. 1. Схема рассматриваемого контейнерного терминала [2]

При разработке модели был смоделирован полный технологический цикл прибытия грузовых универсальных контейнеров на терминал на автомобильном или железнодорожном транспорте, прохождение транспортными средствами пункта пропуска и сверки документации с грузом, размещение контейнеров в очередь на погрузку в зону штабельного хранения с использованием 8-ми ричстакеров, схема обработки штабеля показана на рис. 2.

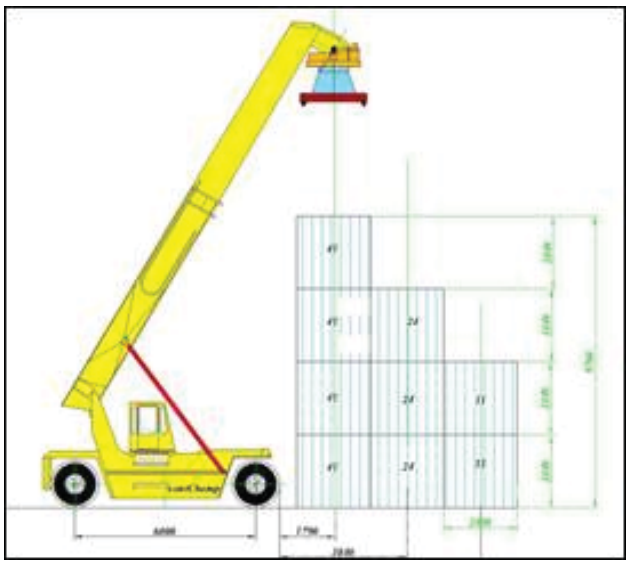


Рис. 2 Схема погрузки/выгрузки контейнера в штабель с использованием ричстакеров

Затем был представлен обратный процесс отправления контейнеров с терминала, начиная с изъятия нужного контейнера из штабеля, подтверждения подлинности документов и их соответствия контейнерному грузу, погрузка на транспорт отправления (автомобиль, железнодорожная платформа) и дальнейшее отправление получателю. Анализ проработанной модели позволил собрать статистические данные входных и выходных потоках поступления грузов на терминал, определить требующееся количество мест хранения контейнеров, рассчитать временные промежутки ожидания перед обработкой и время непосредственной обработки грузов. Адекватность полученных результатов обеспечивалась сопоставлением реальных величин с расчетными.

Далее на базе существующей имитационной модели была предложена усовершенствованная система стеллажного хранения, со своими временными параметрами обработки грузов на каждом этапе, с отличающимся парком ПТО, в качестве которого используются транспортеры-шаттлы и подъемники, что схематично показано на рис. 3 [4].

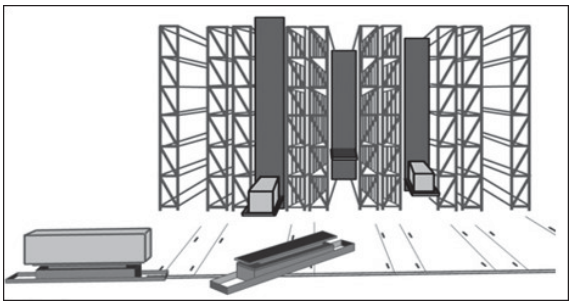


Рис. 3 Схема хранения в стеллажах с использованием автоматических транспортеров [4]

После того как контейнер будет поднят на заданный ярус хранения, специализированная автоматизированная тележка-шаттл переместит контейнер в заданную ячейку хранения. Применение подобного ПТО, время подъема, опускания и передвижения которого зависит лишь от высоты подъема и дальности, имея при этом строго определенные величины, позволяет задавать характеристики объектов потоковой диаграммы с меньшим разбросом значений вероятностных величин. Для реализации данной модели ПТО также будет задано как количество со своими едиными характеристиками.

К параметрам входного потока рассматриваемой модели относятся:

– интенсивность прибытия грузовых контейнеров автомобильным транспортом, TEU/мин; – интенсивность прибытия грузовых контейнеров железнодорожным транспортом, TEU/ч; – количество контейнеров, единовременно поступающих в систему в зависимости от транспорта прибытия, шт.

Выходной поток – это поток заявок, покидающих систему после обслуживания. К параметрам выходного потока рассматриваемой модели относятся: – интенсивность отправления грузовых контейнеров автомобильным транспортом, TEU/мин; – интенсивность отправления грузовых контейнеров железнодорожным транспортом, TEU/ч; – количество контейнеров, единовременно покидающих систему в зависимости от транспорта отправления, шт.

Важно отметить, что для схемы со стеллажным хранением было определено количество подъемно-транспортного оборудования, обеспечивающего требуемую пропускную способность за рассматриваемый период, составляющую 200 000 TEU/год. Если для варианта со штабельным хранением количество единиц оборудования составляло 8 ричстакеров, то для обеспечения производительности системы со стеллажным хранением необходимы 4 подъемника и 4 транспортные тележки.

Реализация экспериментов варьирования параметров. Программа Anylogic позволяет оценить степень и характер влияния интересующих параметров на поведение модели. Для этого на базе разработанной модели реализуется эксперимент варьирования параметров, позволяющий запускать модель заданное количество раз с варьируемыми значениями выбранных параметров.

При прогонах имитационной модели было установлено, что на длину очереди в процессе погрузки контейнеров и на время ожидания погрузки, а также на время размещения контейнеров в склад влияет интенсивность прибытия контейнеров для каждого вида транспорта. Интенсивность отправления в данном случае никакого влияния не оказывает. И, наоборот, на длину очереди при изъятии контейнеров из склада для дальнейшей отправки, на время ожидания в очереди на разгрузку и время самой разгрузки непосредственное влияние оказывает интенсивность отправления контейнеров отдельно для автомобильного и железнодорожного транспорта. Однако в качестве ограничения при проведении эксперимента будет учитываться тот факт, что контейнерные поезда прибывают на терминал по расписанию, которое практически не меняется. Некоторый небольшой разброс указанных величин генерируется по нормальному закону. Это говорит о нецелесообразности варьировать интенсивности прибытия и отправления поездов. Поэтому принято решение при проведении эксперимента варьирования параметров рассматривать влияние интенсивностей прибытия и отправления только автомобильного транспорта и наблюдать за изменениями искомых величин на показатели системы.

Таким образом, эксперимент варьирования параметров состоял из следующих этапов: – варьирование интенсивности прибытия контейнеров на автомобильном транспорте в диапазоне от 1 до 4 TEU/мин; – варьирование интенсивности отправления на автомобильном транспорте в диапазоне от 1 до 12 TEU/мин;

Для каждого варианта исходных данных осуществлялось по 10 прогонов модели с последующим усреднением контролируемых величин. При этом длительность одного прогона составляла 1 месяц или 720 часов. Для построения аппроксимирующих зависимостей показателей функционирования систем был введен коэффициент неравномерности интенсивностей грузопотоков прибытия/отправления грузов, который определялся как отношение интенсивности прибытия к интенсивности отправления контейнеров из склада.

Результаты обработки экспериментов представлены на рисунках 4 – 7.

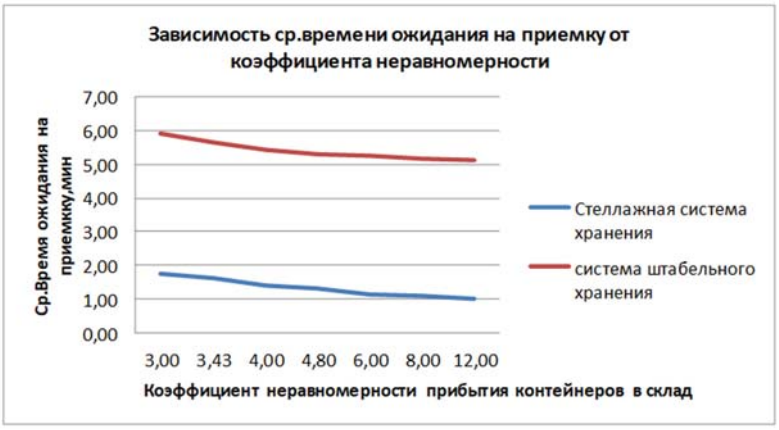


Рис. 4. График зависимость среднего времени ожидания на приемку от коэффициента неравномерности

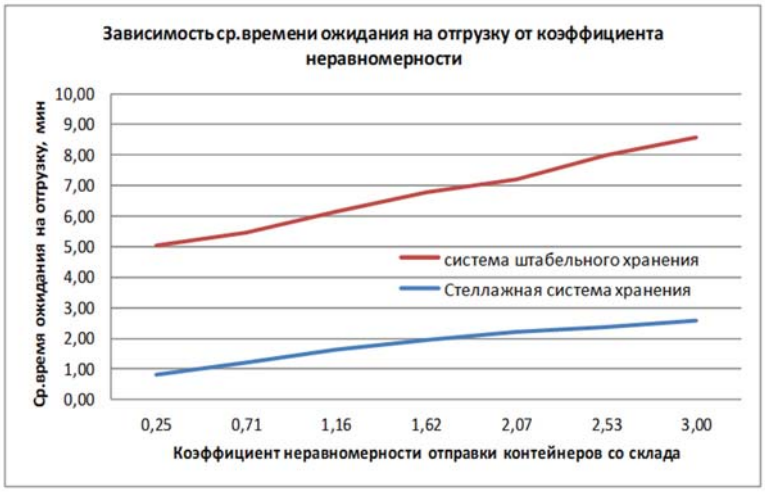


Рис. 5. График зависимость среднего времени ожидания на отправку от коэффициента неравномерности

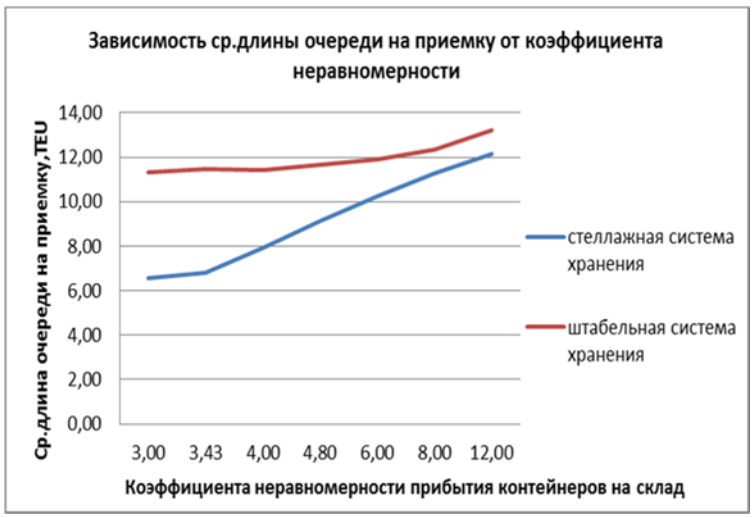


Рис. 6. График зависимость средней длины очереди на приемку от коэффициента неравномерности

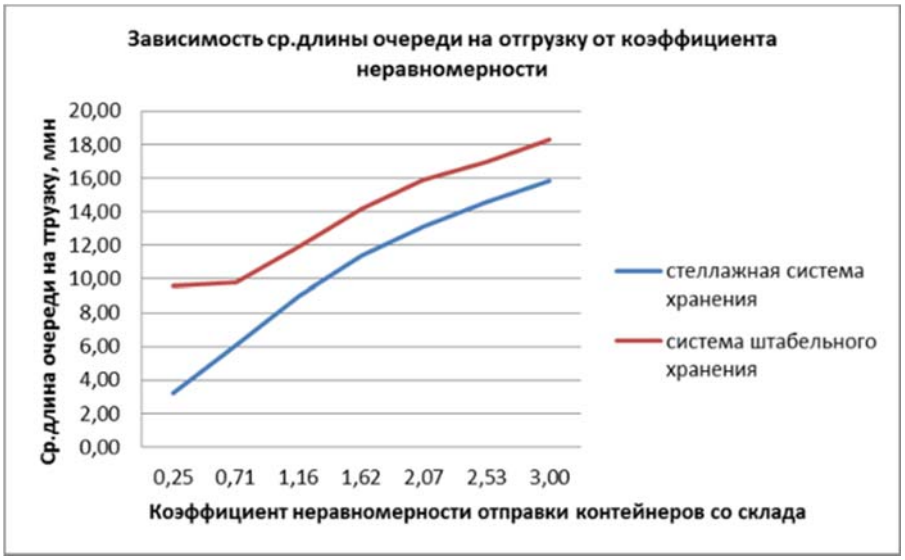


Рис. 7. График зависимости средней длины очереди на отправку от коэффициента неравномерности

Заключение.

При снижении коэффициента неравномерности, т.е. практически при выравнивании интенсивностей прибытия и отправления контейнеров на автомобильном транспорте наблюдается увеличение средней длины очереди на приемку контейнеров в склад, что связано с полной загрузкой оборудования под обслуживание заявок. Применение ПТО с более определенными характеристиками, т.е. с меньшим значением разброса случайной величины времени обслуживания, позволяет сокращать длину очереди при стеллажной системе хранения. Как видно из графиков, представленных на рисунках 4 – 7, чувствительность системы стеллажного хранения к неравномерности грузопотока выше. Однако, в виду того, что система организации складской зоны с применением штабельной системы хранения контейнеров подразумевает наличие вспомогательных операций транспортирования и укладки каждого контейнера в штабель, то могут возникать «конфликтные ситуации». То есть, ситуации, при которых ПТО, задействованное одновременно на участках погрузки и разгрузки автомобильного и железнодорожного транспорта, может быть определено системой или операторами сразу на несколько технологических участков, что невозможно. В таком случае, в качестве рекомендаций необходимо предусмотреть действия для оптимизации размещения контейнеров в штабеле по критерию оборачиваемости поступающих контейнеров с использованием ABC-анализа.

Абсолютно такая же ситуация намечается и с исследованием зависимости средней длины очереди на отгрузку из склада от коэффициента неравномерности грузопотоков только при обратном значении коэффициента. Сравнивая полученные зависимости, можно сделать вывод, что система штабельного хранения менее чувствительна к изменению интенсивности грузопотока. Однако это связано с тем, что в процессе эксперимента наблюдались ситуации, когда одно и тоже ПТО применялось при разгрузке поезда и тут же отправлялось на погрузку контейнера на автомобиль. Отсюда происходит увеличение времени обработки на размещение в складской зоне и отгрузки из нее. Время ожидания в очереди и время обработки грузовых контейнеров варьируются в широких пределах за счет изменяемых параметров техники и условий функционирования самой системы штабельного хранения. Так, например, для изъятия контейнера из глубины

штабеля, погрузчик или ричстакер для начала должен разгрузить ярус, далее оператор определяет, куда расположить снятые грузовые единицы. Подобные дополнительные маневры замедляют полезную производительность процесса, увеличивают время обработки грузов и, как следствие, увеличивают очередь. Применение же системы стеллажного хранения синхронизирует процесс обработки, создает его более ритмичным. Применение такой модели будет целесообразно, если тщательно отладить процесс управления терминалом и внедрить автоматизированные системы контроля.

Анализируя, полученные результаты моделирования можно выделить ключевые преимущества стеллажной системы хранения:

– сведение к минимуму вспомогательных операций транспортировки и обработки контейнеров, предшествующих их размещению в стеллажи;

– синхронизация и ритмичность процесса, позволяющие уменьшать длины очередей на обработку контейнеров и снижать время ожидания на погрузку или разгрузку из склада;

– ускорение оборачиваемости контейнеров;

– сокращение складских площадей, за счет увеличения ярусов складирования и уменьшения проездов ПТО.

СПИСОК ЛИТЕРАТУРЫ

1. Николаевский Н.Н., Пилипчук С.Ф., Спасский Я.Б. Обоснование выбора технологии перегрузочных работ с учетом особенностей функционирования объекта. Логистика и управление цепями поставок. 2017. № 3 (80). С. 21-30.
2. Модуль транспортно-экспедиторская компания, транспортировка грузов, 3PL-сервисы [Электронный ресурс]. URL: http://www.modul.global (дата обращения 01.09.2018);
3. Bladen, Christian Yates, Richard Lackinger. – № EP20070757798; заявл. 02.04.2007; опубл. 25.07.2014.;
4. Kap Hwan Kim, Mai-Ha Thi Phan, Youn Ju Woo. New Conceptual Handling Systems in Container Terminals. Vol 11, No 4, December 2012, pp.299309.;
5. Патент США №3836020, МПК B65G 1/06. Container/cargo handling plant/ H. Lassig; патентообладатель Firma Fördertechnik Hamburg; заявл. 12.04.1973; опубл. 17.09.1974.;
6. Патент США № EP2146894, МПК B65G 67/60, B63B 27/00. Port storage and distribution system for international shipping container/ заявитель и патентообладатель Charles Benedict, Brian Pfeifer, James Dobbs, Scott Vatanabe I. Port development. A handbook for planners in developing countries.:Great Britain,2001-243 p.;
7. Патент EP №1539619, МПК B65G 39/00. Verfahren zum be- und entladen/ Helmut Klaus Schimany, Dietmar Schratt; заявитель и патентообладатель Rail Cargo Austria AG. -№ EP20030794681; заявл. 09.09.2003; опубл. 15.06.2005

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

УДК 681.3.06

УСЛОВИЯ ИНФОРМАТИЗАЦИИ ПЕРСПЕКТИВНЫХ СИСТЕМ ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ ПРАКТИЧЕСКОЙ ПОДГОТОВКОЙ

Алексеев Сергей Алексеевич, Парфенов Николай Петрович, Стахно Роман Евгеньевич, Яковлева Наталья Александровна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: ksgati@yandex.ru

Аннотация. Выявленные основные особенности развития профессиональной подготовки будущих специалистов в учебных заведениях, в том числе и практической подготовки с использованием технических средств обучения, позволили определить структуру и содержание практической подготовки, которая должна удовлетворять организационным и дидактическим требованиям к ее эффективности. Содержание практической подготовки должно быть направлено на совершенствование ее качественных параметров. В настоящее время отработка умений и навыков в ходе практической подготовки не создает у обучаемых целостного представления о будущей профессиональной деятельности. Эффективность практической подготовки определяют три вида «человеческого фактора»: результаты профотбора кандидатов на обучение, аттестационные характеристики выпускников и педагогическое мастерство руководителей занятия.

Ключевые слова: эффективность; организационное управление; образовательная система; комплекс средств автоматизации.

THE CONDITIONS OF INFORMATIZATION OF PROMISING SYSTEMS OF ORGANIZATIONAL MANAGEMENT PRACTICAL TRAINING

Alekseev Sergey, Parfenov Nikolay, Sakhno Roman, Yakovleva Natalia
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mail: ksgati@yandex.ru

Abstract. The main features of the development of professional training of future specialists in educational institutions, including practical training using technical means of training, allowed to determine the structure and content of practical training that must meet organizational and didactic requirements for its effectiveness. The content of practical training should be aimed at improving its quality. Currently, the development of skills in the course of practical training does not create a holistic view of the trainees ' future professional activities. The effectiveness of practical training is determined by three types of «human factor»: the results of professional selection of candidates for training, certification characteristics of graduates and pedagogical skills of managers.

Keywords: efficiency; organizational management; educational system; complex automation.

Введение.

Ликвидация многих негативных явлений в области практической подготовки (ПП) будущих специалистов связана с созданием системы организационного управления (СОУ) ПП. Для рассмотрения существующих подходов, принципов и методов проектирования по информатизации, обеспечивая СОУ объектами различных классов и назначений, необходимо уточнить ряд понятий и определений (тезаурус).

На основании данного тезауруса могут быть сформированы основные определения, относящиеся к предметной области проектирования по информатизации СОУ ПП:

– Организационное проектирование − это управленческая деятельность, направленная на определение моделей оптимальных систем управления, их основных характеристик, параметров, качеств и критериев это упорядочение организационно-структурных характеристик системы для достижения поставленных целей или повышения ее эффективности с точки зрения реализации поставленных задач.

– Эффективность − отношение эффекта, результата к затратам, расходам, обусловившим, обеспечившим его получение.

– Качество − совокупность свойств, параметров и характеристик объекта, обеспечивающая его способность удовлетворять планируемым или установленным требованиям.

– Свойство − сторона объекта (процесса, явления), определяющая его сходство или различие с другим объектом (процессом, явлением) и обнаруживается в его отношении к ним.

– Характеристика – взаимосвязь между независимыми и зависимыми переменными, характеризующими объект (явление, процесс), выраженная содержательно или аналитически.

– Процесс управления – процесс целенаправленного перевода объекта (явления, процесса) из одного состояния в другое путем воздействия на него субъекта управления.

– Организационное управление – процесс организационного воздействия, направленный на достижения целей посредством упорядочения преобразований исходных ресурсов в требуемые результаты.

– Цель управления – планируемое (возможное или желаемое) состояние объекта управления, в которое его необходимо перевести в результате управляющих воздействий со стороны системы управления. т.е. это состояние должно быть достигнуто.

– Цель организационного проектирования – придание процессу новых или развитию действующих систем целенаправленности и научной обоснованности.

– Проектирование системы управления – процесс создания новой системы управления на основе достижений науки и техники или модернизации существующей на основе нейтрализации выявленных недостатков или за счет выявления новых задач управления и/или требований к эффективности их решения.

– Процесс организационного проектирования – целенаправленная последовательность актов принятия проектных решений, приводящая к построению проектируемой организационной системы (реализация процесса организационного проектирования требует использования соответствующей информационной технологии).

– Система организационного управления практической подготовкой – целостная совокупность функционально-связанных структурных компонент, осуществляющих комплексное, координированное и планомерное управляющее воздействие на систему (процесс) практической подготовки с целью гарантированного выполнения госзаказа на практическую подготовку будущих специалистов с требуемыми показателями эффективности.

Приведенные понятия и определения позволяют сформулировать основные условия проектирования по информатизации ОУ ПП:

– первое – обязательно наличие четко определенной цели управления ПП и критериев ее достижения в ходе реализации процесса управления,

– второе – наличие некоторого количества альтернативных методов управления ПП,

– третье – возможность определения точной и достоверной оценки последствий осуществления каждой из альтернатив как с точки зрения результативности ОУ ПП, так и оперативности, и затрат различного рода ресурсов с учетом существующих ограничений.

– Кроме того, должны быть определены основные принципы ОУ ПП, исходя из следующих соображений:

– процесс ПП будущих операторов в учебных заведениях нуждается в создании специального инструментария для оценивания его эффективности,

– существующее рассогласование между эффективностью ПП выпускников учебных заведений и требованиями к ним, определяемыми реальной практикой их профессиональной деятельности после выпуска, обуславливает необходимость разработки достаточно универсального методического аппарата, позволяющего управлять уровнем практической подготовленности выпускников к решению профессиональных задач,

– в рамках общей задачи совершенствования ПП задача проектирования СОУ ПП является самостоятельной, на базе которой должны решаться другие задачи.

На рис. 1 отражена взаимосвязь процедур проектирования СОУ ПП и организации процесса ПП.

Рис. 1. Правила построения и содержание процедур проектирования системы организационного управления практической подготовкой

При проектировании по информатизации СОУ ПП и определении организации самого процесса ОУ ПП необходимо устанавливать на основе руководящих документов требования как к эффективности

функционирования названной системы, так и к эффективности организации процесса управления. Кроме того, должны быть определены виды частных и интегральных показателей оценивания эффективности СОУ ПП и эффективности организации процесса управления.

В состав принципов ОУ ПП следует включить [1, 2, 5]:

1. Принцип системности (целостности), который определяет такое построение процесса организационного управления подготовкой и такую структуру СОУ ПП, при которых управление всеми элементами системы ПП должно рассматриваться как комплекс субъектов и объектов управления, взаимосвязанных и согласованных по цели, времени и месту взаимодействий с учетом их принадлежности к системе ПП.

2. Принцип плановости управления, который определяет необходимость планирования последовательности управляющих воздействий на процесс ПП со стороны СОУ ПП, что позволит путем моделирования оценить возможные результаты и методы их достижения.

3. Принцип эффективности управления, который определяет требования сравнения конкурирующих вариантов ОУ ПП с помощью, проектируемой СОУ ПП с использованием набора критериев и показателей, позволяющих оценить каждый вариант управления по результативности, оперативности и ресурсозатратам.

4. Принцип оптимальности, который определяет, что организационное управление ПП с использованием СОУ ПП не только отвечает требованиям эффективности и имеет заведомо запланированный характер, но и то, что совокупность управляющих воздействий должна обеспечивать наилучший (оптимальный) результат управления, приводящий к повышению эффективности ПП.

Чтобы проектируемая СОУ ПП была целостной, плановой, эффективной и оптимальной, в общем случае она должна включать в свой состав две подсистемы [3, 5]: организационную и дидактическую, взаимодействие которых показано на рис. 2.

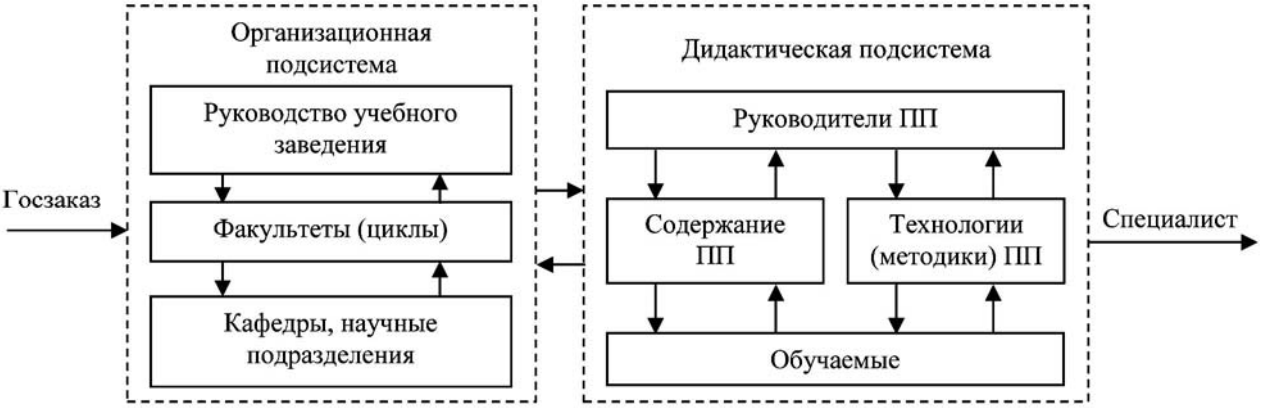


Рис. 2. Взаимодействие подсистем СОУ ПП

Из рисунка 2 следует, что внутри каждой подсистемы имеют место прямые и обратные связи, аналогичные связи объединяют обе системы. Прямые связи в организационной подсистеме реализуются сверху вниз по уровням иерархии управления в виде приказов, руководящих указаний, планов и т.д. Обратные связи – доклады, отчеты, акты работы комиссий, в том числе Государственной аттестационной комиссии. Прямые связи в дидактической подсистеме – это управляющие воздействия руководителей ПП на обучающихся через содержание и технологии (методики) ПП, приводящие к формированию умений и навыков, а также к выработке требуемых личностных характеристик будущих специалистов. Обратные связи в дидактической подсистеме позволяют корректировать управляющие воздействия, содержание и технологии ПП. Прямые связи между подсистемами реализуются через информационные технологии к будущему специалисту, определяющие программы ПП. По каналам обратной связи поступает информация об эффективности ПП (текущей, рубежной, итоговой) на основе анализа ее результатов.

Исходя из анализа имеемых прямых и обратных связей, можно дать определение СОУ ПП: это целостная совокупность функционально-связанных структурных компонент, осуществляющих комплексное, координированное и планомерное управляющее воздействие на систему (процесс) ПП с целью гарантированного выполнения госзаказа на практическую подготовку будущих специалистов с требуемыми показателями эффективности.

Основой управляющих воздействий является информация о всех состояниях, целях, средствах и условиях функционирования каждого элемента системы (процесса) ПП, отсюда обязательным условием является возможность измерения количественных и качественных параметров этих элементов на любом этапе управления [1, 3, 4].

Если применить современный подход к ОУ ПП, то этот процесс можно декомпозировать на последовательность следующих этапов (рис. 3): 1) развертывание функции эффективности ПП; 2) разработка модели эффективности ПП; 3) управление эффективностью ПП; 4) совершенствование процесса ОУ ПП.

Рис. 3. Основные этапы процесса ОУ ПП

В настоящее время в существующих системах ПП практически реализуются все четыре этапа. При этом реализация второго и третьего этапов осуществляется традиционным способом: по четырехбальной шкале оценивается результат ПП, т.е. контролируется и оценивается ее конечный результат в виде фиксации достигнутого уровня умений и навыков обучающихся. Названные контроль и оценивание либо осуществляются субъективно (на основании опыта) руководителями ПП, либо используются автоматизированные системы оценивания деятельности обучающихся.

В перспективных СОУ ПП необходимо осуществить переход к контролю и оцениванию всех элементов, функционирующих в рамках системы и ее подсистем. Иными словами, необходимо контролировать и оценивать целостный процесс ПП, характеристики которого позволяют оценить реальную и потенциальную эффективности ПП.

Следовательно, в перспективных СОУ ПП, (в отличие от существующих, в которых используются критерии и показатели (чаще всего традиционная бальная система) успешности ПП обучающихся при текущем, рубежном и итоговом контроле) должны использоваться критерии и показатели оценивания эффективности функционирования всех элементов системы ПП.

Необходимо отметить, что эффективность ПП будущих специалистов в учебных заведениях, как и эффективность самого процесса ПП, зависит от большого числа объективных и субъективных факторов. Ясно, что не все факторы могут быть учтены при построении частных и обобщенной моделей СОУ ПП (этап 2, рис. 3), т.к. учет большого числа разнородных факторов и их взаимосвязей неизбежно приведет к значительному усложнению названных моделей и существенно сузит их практическое применение. При этом следует подчеркнуть, что основным требованием к моделям СОУ ПП является их открытость, определяющая возможность их коррекции и дополнения с учетом изменения требований, целей или условий проведения ПП.

В итоге можно констатировать, что создание перспективных СОУ ПП предполагает решение следующих задач проектирования:

– 1) построение частных и обобщенной моделей ОУ ПП, адекватно описывающих условия реализации мероприятий ПП;

– 2) учет динамики изменения требований к профессиональным и личностным характеристикам выпускников по соответствующим специальностям;

– 3) создание методов и средств для получения объективного количественного оценивания значений показателей эффективности всех элементов системы ПП;

– 4) разработка научно-методического аппарата прогнозирования изменения эффективности ПП будущих специалистов в результате управляющих воздействий СОУ ПП на элементы системы ПП.

Решение перечисленных задач проектирования по информатизации СОУ ПП требует применения новых информационных технологий и современных средств автоматизации. Их отсутствие, даже если будут созданы адекватные, валидные и верифицированные модели и методы оценивания и регулирования процесса ПП, не позволит внедрять на практике новые методы ОУ ПП, а следовательно, перейти от существующей к перспективной СОУ ПП. Таким образом, одним из необходимых условий проектирования и реализации

перспективной СОУ ПП, наряду с созданием эффективных методов моделирования и оценивания эффективности ПП, является разработка на базе современных информационных технологий с использованием элементов искусственного интеллекта (ИИ) и внедрение автоматизированной СОУ ПП с целью повышения эффективности ОУ ПП.

Заключение.

Анализ структуры и функций тренажерных средств (ТС), как ТСО специального назначения, при подготовке специалистов показал следующее: 1) структура специализированных и комплексных ТС имеет явно выраженный модульный характер; 2) отсутствуют четкие алгоритмы обоснования психолого-педагогических требований к эффективности ТС при их проектировании; 3) типовой состав практически любого ТС позволяет реализовать сам процесс ПП, но без управления ее эффективностью; 4) перспективными ТС являются ТСО; 5) ТС составляют основу ТСО, обеспечивающую ПП, что приводит к необходимости определения требуемого набора ТС для конкретного вида ПП.

Сформулированы основные условия синтеза СОУ ПП с использованием тезауруса и основные принципы ОУ ПП. Разработана схема взаимосвязи процедур проектирования СОУ ПП и организации процесса ПП. Обосновано, что СОУ ПП должна включать две подсистемы:

– организационную, куда входят руководство учебного заведения, факультеты (циклы), кафедры, научно-исследовательские лаборатории;

– дидактическую, включающую руководителей ПП, обучаемых, содержание и технологии (методики) ПП.

Установлено, что процесс ОУ ПП включает последовательность этапов:

– развертывание функции эффективности ПП,
– построение структурно-функциональной модели ОУ ПП,
– ОУ ПП на основе модели,
– совершенствование процесса ОУ ПП.

Предложено в перспективных СОУ ПП осуществлять переход к контролю и оцениванию всех объектов, функционирующих в рамках системы и в ее подсистемах. Для этого необходимо сформировать совокупность единичных, групповых и интегральных показателей и определить поле значимых факторов, влияющих на них.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев С.А., Стахно Р.Е. Вопросы организационного управления содержанием практической подготовки в вузах МВД. // Проблемы современной науки и образования № 19 (101). Москва. изд. «Проблемы науки». 2017. С. 19-22.
2. Алексеев С.А., Гончар А.А., Стахно Р.Е. Основы квалиметрии, автоматизации и интеллектуализации систем организационного управления практической подготовкой в вузах МВД. // Наука, техника и образование. № 5 (35) Москва. изд. «Проблемы науки». 2017. С. 29-32.
1. Алексеев С.А., Гончар А.А., Стахно Р.Е. Моделирование структуры и процесса организационного управления тренажерной подготовкой в образовательных учреждениях правоохранительных органов.// Журнал «Вестник полиции» 5(1) - 2018 г., С. 3-9.
2. Низамов М.М. Концептуальная модель совершенствования ТСО вуза МЧС России: Материалы X Международной конференции «Современные технологии обучения СТО-2004». – СПб.: СПбГЭТУ – «ЛЭТИ», 2004. – С. 93-95
3. Багрецов С.А. Квалиметрия групповой деятельности операторов сложных систем управления: под ред. Б.С. Алешина. – М.: Физматлит, 2006. – 384 с.: ил.

УДК 004.4

ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ ПРИ СОЗДАНИИ ДОКУМЕНТОВ С ИСПОЛЬЗОВАНИЕМ MS OFFICE

Домбровская Лариса Александровна, Гончар Артем Александрович, Яковлева Наталья Александровна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: dombr-21@mail.ru, gonchar.tema@yandex.ru, kumirova@mail.ru

Аннотация. Рассматриваются различные методы и приемы автоматизации при создании текстовых документов с использованием возможностей MS Office.

Ключевые слова: автоматизация; шаблон документа; слияние документов; технология стилей; автозамена, технология макросов.

AUTOMATION TECHNOLOGIES FOR CREATING DOCUMENTS USING MS OFFICE

Dombrovskaya Larisa, Gonchar Artem, Yakovleva Natalia
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mail: dombr-21@mail.ru, gonchar.tema@yandex.ru, kumirova@mail.ru

Abstract. Various methods and methods of automation are considered when creating text documents using the capabilities of MS Office.

Keywords: automation; document template; document merging; style technology; auto-replacement; macro technology.

Современная профессиональная деятельность тесно связана с различного рода информацией, её поиском, использованием, обменом и сохранением.

Автоматизация этих процессов повышает их эффективность. Применение технических и программных средств, внедрение в практику современных методов работы с информацией позволяют повысить надежность, достоверность, доступность и разнообразие используемой информации, а также ускорить работу с ней.

Современная программная индустрия предлагает самые разнообразные средства работы с информацией – получения, хранения, обработки, обмена, организации совместной работы и т.д. Многие технологии включаются и в самые распространенные офисные приложения, это значит, что они имеются на большинстве компьютеров и доступны. Однако доля использования этих технологий очень незначительна, одной из причин этого является низкая осведомленность пользователей об их существовании и возможностях.

Компьютер часто используется как пишущая машинка, и скорость работы с ним определяется только нервной организацией пользователя и его навыками работы с клавиатурой и типовыми средствами, имеющимися в программах.

В офисных программах реализуется комплексный подход к решению круга задач работы с документами. Преимуществом этих программ является их универсальность и распространенность. Это означает и совместимость документов, подготовленных на разных компьютерах, и подготовленность пользователей работать с такими документами. Кроме этого, в этих программах закладываются значительные возможности, которыми большинство пользователей могут и не применять, и даже не знают о них.

Идеального решения использования всего круга заложенных в офисных программах средств нет. Однако некоторые технологии, позволяющие повысить эффективность работы с документами, могут быть взяты для использования и позволят пользователю более уверенно работать с документом на всех этапах: от его создания, редактирования, форматирования до конечного варианта электронной верстки.

Ряд направлений и задач, в которых может быть существенно повышена эффективность работы с информацией, а также технологии, которые обеспечивают такое повышение, рассматриваются далее.

Организация совместной эффективной работы с разделяемой информацией. Задача совместной работы двух или более человек с одним документом возникает часто. Процессы доступа к общей информации для определенного круга лиц могут быть автоматизированы с помощью соответствующих программных средств.

В распространенном пакете MS Office функция обеспечивается технологией Share Point [3]. Поддерживаются различные стратегии совместного доступа. Автоматизация обеспечивает работу с одной копией документа, возможно сохраняя историю его версий.

При простейшей стратегии файл извлекается с сервера для монопольного использования, а затем возвращается. Во время использования другие пользователи его изменять не могут, только читать. Новая версия файла появится для них после того, как редактор ее возвращает. Отслеживаются и разрешаются возможные конфликты версий у пользователей. Доступ к новой версии может быть подтвержден или отклонен сотрудником, который имеет разрешения на утверждение изменений файлов.

С извлеченным файлом можно просто работать с помощью приложения MS Office – это чаще всего быстрее, чем на сервере управления документами, и не требует серверного соединения.

Другой упрощенный сценарий связан с наличием автора файла, который разрешает другим выполнить для него рецензирование и комментирование, однако за окончательную публикацию документа отвечает сам.

Формальное совместное редактирование позволяет одновременно вносить изменения в документы. Сценарий предполагает, что вносимые авторами изменения буферизуются и обнаруживаются другими пользователями только тогда, когда сохраняются явным образом. При совместном редактировании каждый пользователь видит, в какие части документа вносят изменения его коллеги, в этом ему помогают значки, индикаторы строки состояния и области навигации документа или презентации.

Подробно пошаговое использование средства описано в справке MS Office [4]. Средство относится к профессиональным коммерческим продуктам. Часть программ и компонентов, которые его обеспечивают, являются платными. Например, для управления документами на сервере требуется операционная система линейки Windows Server. Платным является и компонент Microsoft SharePoint Server для интеграции функциональности SharePoint в работу приложений MS Office. Это обстоятельство затрудняет малобюджетное обучение этим технологиям.

Напротив, предметом обучения для обсуждаемых технологий наиболее подходит работа с документами Google. В настоящее время средство является свободным, относится к облачным технологиям, то есть от пользователя конкретная его реализация скрыта, он представляет себе доступные ресурсы как файловую систему. Как и где физически располагаются его данные, пользователь не знает.

Владелец диска Google должен иметь почту на Google mail (gmail.com). Остальные пользователи, которые предполагают одновременно работать с этим диском, должны иметь доступ в Интернет с помощью любого браузера. Доступом управляет владелец диска. Технология Google также не лишена недостатков. Например, преобразует в документы Google документы MS Office не всех форматов. Однако организация совместной работы дает преимущества в эффективности работы в целом.

Использование шаблонов документов. Шаблон – документ, используемый в качестве образца для создания новых документов. В нем могут быть определены различные стили, сочетания клавиш и макросы, настроены параметры страницы, подготовлен определенный текст, который должен содержаться в документе. То есть, часть работы по вводу, оформлению конкретного типа документа и подготовке средства работы с ним уже проделана.

Например, при частой подготовке рапортов на имя начальника, можно создать шаблон такого рапорта.

В Word входят коллекции сотен готовых шаблонов, которые могут быть использованы для создания документов различных типов, часть из них динамически загружается с сайта компании Microsoft и предлагается с помощью меню. Однако в практике каждой организации используют документы совершенно определенного вида, которые, как правило, отсутствуют в коллекции. Этот недостаток исправляется подготовкой комплекта шаблонов всех типов документов, которые используются в практике документооборота подразделений.

Шаблоны можно открывать так же, как и обычные документы. В отличие от обычных файлов, шаблоны не позволяют просто изменять себя. После изменения, если изменения нужно сохранить, будет предложено ввести имя файла типа документ. Для того, чтобы изменить все-таки сам используемый шаблон, указывают это в типе «Шаблон Word».

Такой алгоритм работы с шаблонами организует пользователей и существенно ускоряет работу по созданию типовых документов. Кроме этого, полученные с помощью этой технологии документы выглядят совершенно единообразно. Поэтому комплект шаблонов может быть подготовлен в организации централизованно и им могут обеспечиваться все подразделения.

Рассылка (технологии слияния документов). Часто существует необходимость подготовить массовую рассылку документов, отличающихся друг от друга незначительно. Например, уведомления или поздравления с праздником для группы сотрудников, справки о доходах за год для всех сотрудников. Для этих задач трудоемким является заполнение данных отдельных сотрудников и распечатка полученных результатов. Для случая, когда такие данные имеются в отдельном документе в электронном виде, задача решается быстро путем слияния документа с данными из другого файла.

Одни и те же данные могут быть использованы для подготовки большого числа документов слияния. Имеется возможность применять правила, например, позволяющие генерировать различные тексты в зависимости от значений данных, отбирать записи из файла с данными.

Технология стилей. На крупных сайтах в Интернете часто имеется возможность выбрать пользователю тот вид, в котором ему будут показываться материалы и само оформление сайта. Например, некоторые люди имеют проблемы со зрением, и им нужен более крупный шрифт; для других важна контрастная цветовая схема текста. Некоторые люди хотят отпечатать текст и должны иметь возможность представить его без лишних элементов – рекламы, фона, ссылок и т.д.

Все это достигается не тем, что изготавливается некоторое количество разных вариантов текста. Текст используется один и тот же. А варианты оформления, действительно, представлены в виде набора стилей – специальных таблиц, в которых содержатся все параметры шрифтов, абзацев и т.д. для различных элементов текста. Текст отображается в соответствии с загруженной в данный момент таблицей стилей.

Такой подход отражает общую тенденцию для работы с документами: разделять процесс редактирования (ввода и исправления) текста и его оформления, отказаться от физического форматирования (когда конкретный формат вручную приписывается какому-либо элементу – размер шрифта, выравнивание и границы абзаца).

Вместо этого используют логическое форматирование, когда элементу приписывают не определенные параметры, а только ссылку на стиль, на его имя.

Стиль представляет собой совокупность параметров оформления, которые определяют, как будет выглядеть элемент, Если в дальнейшем стиль изменить, то по-другому начнут отображаться и оформленные с его помощью тексты.

Удобным является закрепление за некоторыми наиболее часто используемыми стилями сочетаний клавиш.

Технологии макросов. В некоторых случаях обработка документа может быть сложной, объемной и проводиться для целого ряда документов. Для офисных приложений можно сохранять все действия, которые делаются для одного файла, и в дальнейшем автоматически выполнять их для других.

Это достигается использованием макросов.

Макрос – программа, записанная на языке программирования, которая служит для автоматизации типичных задач. Программа может быть создана автоматически при включении режима записи макроса. В этом режиме все действия пользователей будут записываться, поэтому нужно быть аккуратным, чтобы не выполнить ненужных действий – например, переключений в другое приложение: в момент, когда будет выполняться макрос, это приложение может не быть загруженным.

При записи макроса команды работы мыши с текстом (выделения, позиционирования) не действуют: в момент, когда макрос будет выполняться впоследствии, на экране будет другой текст, с другими координатами. Команд меню, вместе с тем, с помощью мыши выполняются.

Технологии замены. Во всех текстовых редакторах включены средства автоматизации поиска и замены, позволяющие повысить эффективность работы особенно с документами большого объема, когда заменяемый контекст должен быть изменен большое число раз (десятки, сотни и тысячи), или когда для поиска заменяемого контекста нужно просмотреть значительные объемы текста. Эти средства полезны и для использования в макросах и дают возможность производить сложную замену в большом количестве файлов (типичная скорость обработки – один файл в секунду).

Существенно эффективность средства повышает использования в операциях замены специальных символов, подстановочных знаков и – особенно – регулярных выражений [2].

Технология автозамены. Позволяет при вводе устранять некоторые типичные ошибки, которые образуются при быстром наборе текста. Например, если первые две буквы предложения оказались прописными. Специальной

команды автозамены нет. Настройка ее параметров функции позволяет посмотреть и изменить все возможности автозамены.

В каждой работе существует набор часто применяемых словосочетаний, которые можно включить в таблицу автозамены, и при вводе аббревиатуры она будет заменяться словосочетаниями.

Например, аббревиатуру «ОВД» можно автоматически заменять на «органов внутренних дел». Правда, при этом в некоторых версиях MS Word могут быть сложности с набором, например, такого слова, как «овдовевший».

В статье рассмотрены наиболее востребованные практикой технологии, применяемые при изучении таких дисциплин как «Информатика и информационные технологии в профессиональной деятельности», «Информатика», «Информационные технологии в юридической деятельности» и других в Санкт-Петербургском университете МВД России.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО 15489-1-2007 Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования.
2. Ноэл Майкл, Спенс Колин Microsoft SharePoint 2007. Полное руководство. – М.: Вильямс, 2008.
3. http://office.microsoft.com/ru-ru/sharepoint-server-help/HA101812148.aspx
4. Отчет о научно-исследовательской работе по теме: Технологии создания юридических документов с использованием MS Office: Учебное пособие. – СПб.: СПб. ун-т МВД России, 2013. – Электронный документ.

УДК 37.1

РАЗВИТИЕ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАМКАХ ДВИЖЕНИЯ WORLDSKILLS В ТЕХНИКУМЕ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Голубева Ольга Павловна
Санкт-Петербургский техникум железнодорожного транспорта – структурное подразделение Петербургского университета путей сообщения Императора Александра I
Бородинская ул., 6, Санкт-Петербург, 191180, Россия
e-mail: olgapavna2016@gmail.com

Аннотация. Предложены способы применения высокотехнологичных компьютерных технологий для проведения демонстрационного экзамена по системе Worldskills. Рассматриваются методы и средства имитационного моделирования, используемые для построения цифровой образовательной среды для поддержки учебного процесса подготовки специалистов среднего звена.

Ключевые слова: информатизация образования; цифровая информационная образовательная среды; демонстрационный экзамен WORLDSKILLS; среднее профессиональное образование.

INFORMATION TECHNOLOGY DEMO EXAM WORLDSKILLS THE COLLEGE OF RAILWAY TRANSPORT

Golubeva Olga
The St. Petersburg Railway Technical School - Structural Subdivision of Emperor Alexander I St. Petersburg State Transport University
6 Borodonskaya Str., St. Petersburg, 191180, Russia
e-mail: olgapavna2016@gmail.com

Abstract. The ways of application of high-tech computer technologies for the demonstration exam system Worldskills. The methods and means of simulation used to build such an educational environment to support the educational process of training middle managers are considered.

Keywords: computerization of education; e-learning environment; demonstration exam; secondary vocational education.

Введение.

Российская система образования присоединилась к движению WorldSkills в 2012 году. В тот период техникумы и колледжи, несмотря на попытки непрерывных реформ, по-прежнему казались многим абитуриентам не престижной образовательной ступенью, на которую ориентируются те, кому не удалось поступить в высшее учебное заведение и те, кто не готов к единому государственному экзамену (ЕГЭ) [1].

В реформировании системы среднего профессионального образования участвует общественная организация, развившаяся в общественное движение Союз «Молодые профессионалы (Ворлдскиллс Россия)». Особенность российской структуры WorldSkills состоит в том, что она ориентирована на реформирование всей системы профессионального образования, а не только отдельных направлений подготовки. Для государственных структур образования WorldSkills обеспечивает 1) рейтинг образовательных организаций по качеству профессиональной подготовки кадров; 2) анализ содержания образовательных программ; 3) оценку уровня квалификации педагогических кадров и другие управленческие функции, такие, как например, открытость образования, связь с обществом, с работодателями, с семьей, с родителями и др.

Для обеспечения конкурентоспособности выпускников на рынке труда проводится демонстрационный экзамен, который принимают эксперты WorldSkills. На этом экзамене студенты выполняют задания, разработанные экспертным сообществом WorldSkills. Важно отметить, что демонстрационный экзамен по требованиям движения Worldskils проводится на реальных производственных объектах с применением действующего технологического оборудования и включает задания. Например, задание маршрута в режиме АРМ ДНЦ возможно двумя способами: задать маршрут поезду в режиме поездного диспетчера (ДНЦ) возможно двумя способами: курсором по попутным и встречным светофорам, либо нажатием от первого светофора до повторителя прибывающего поезда. Выбор обучающимся второго способа действия показывает более сформированную компетенцию действий поездного диспетчера, чем дежурного по станции. Второй: на уровне оценки сформированности компетенций более высокого уровня действий работников, обеспечивающих перевозочный процесс, задания сформулированы с целью организовать безопасный пропуск поездов по станции в условиях нарушения нормальной работы устройств сигнализации, централизации и блокировки (СЦБ).

На данном этапе свыше 14 000 студентов и выпускников профессиональных образовательных организаций сдали демонстрационный экзамен по 73 компетенциям. В пилотном проекте приняли участие 26 регионов России. При отборе регионов учитывался опыт проведения в субъекте региональных чемпионатов, демонстрационного экзамена в 2017 году, участие в реализации проекта по внедрению регионального стандарта кадрового обеспечения промышленного роста, наличие у колледжей, лицеев и техникумов статуса специализированных центров компетенций WorldSkills и готовность предприятий региона участвовать в организации и проведении демонстрационного экзамена по соответствующей компетенции [2].

Осуществление подготовки к демонстрационному экзамену на реальном оборудовании достаточно сложно и травмоопасно. Это предполагает исследование эффективности применения компьютерных технологий при подготовке, организации и проведении демонстрационного экзамена по существующим в WorldSkills стандартам.

Анализ задач пилотного проекта по внедрению демонстрационного экзамена по стандартам WorldSkills Russia в систему государственной итоговой аттестации в январе 2017 года по некоторым компетенциям профессионального образования, в число которых включили компетенцию «Организация движения поездов локомотивными бригадами», показывает, что компетенции других профессий обеспечения перевозочного процесса на железнодорожном транспорте также могут проверяться на демонстрационном экзамене.

Санкт-Петербургский техникум железнодорожного транспорта осуществляет подготовку техника по организации перевозок и управлению на транспорте по рабочим профессиям сигналиста, приемосдатчика груза и багажа, составителя поездов. В учебном процессе используются традиционные методы обучения, среди которых преобладают словесные методы и наглядные, оценка компетенций происходит с использованием контрольных работ, вопросов и заданий на зачетах и экзаменах в устной форме. Следует отметить, что это позволяет сформировать систему профессиональных знаний, но недостаточно практических заданий, которые можно выполнить на современном оборудовании. Студенты с трудом интегрируют полученные теоретические знания и практические умения для выполнения конкретных действий в своей профессиональной деятельности дежурного железнодорожной станции, приемосдатчика груза и багажа и т.п.

Наш опыт показал, что формированию профессиональных компетенций техников возможно с использованием инструментария информационных технологий и интеллектуальной высокотехнологической образовательной среды. Она позволяет повысить мотивацию деятельности от сознаваемой к реальной, действующей при выполнении профессиональных функций, в том числе и на демонстрационном экзамене.

Ведущей составляющей такой среды является комплекс тренажеров на базе современной вычислительной техники в составе лаборатории управления движением, в том числе, программно-технический комплекс «Имитационный тренажер ДСП/ДНЦ» с табло коллективного пользования, имитационный 3D-тренажер для приемосдатчиков груза и багажа, и приемщиков поездов. Оборудование было предоставлено открытым акционерным обществом «Российские железные дороги» - основным работодателем выпускников техникума.

На экране в кадре реального состояния инфраструктуры и поездного положения имитируется движение в режиме нормальной безаварийной эксплуатации. В начале обучения студенты индивидуально (каждый на своей станции) отрабатывают порядок действий, в соответствии с требованиями к конкретной должности работника на станции. Система вычисляет число ошибок и неправильных действий, отсылает к аналогичным заданиям. Студент обязан выполнять операции по осуществлению перевозочного процесса с применением современных информационных технологий управления перевозками, что соответствует профессиональной компетенции (ПК 1.1). Затем ситуация усложняется нештатными, сбойными и аварийными ситуациями. При этом действие на экране сопровождается имитатором звука реальных устройств, фотографиями, анимацией и закадровым текстом, поясняющим смысл нештатной ситуации, установленный порядок действий работников дирекций перевозок и смежных служб, которые участвуют в устранении возникшей нестандартной ситуации. Это способствует освоению компетенции по организации работы персонала по обеспечению безопасности перевозок и выбору оптимальных решений при работах в условиях нестандартных и аварийных ситуациях (ПК 1.2).

С целью обеспечения безопасности движения и решения профессиональных задач посредством применения нормативно-правовых документов (ПК 2.2) система поддерживает программу обучения правильному ведению журнала осмотра формы ДУ-46. На экране происходит его поэтапное (пошаговое)

заполнение, которое комментируется закадровым звуковым сопровождением. Кроме того, имитируется ведение переговоров между поездным диспетчером, дежурным по станции, машинистом поезда и другими работниками.

Опыт показывает, что решение задач на тренажере позволяет сформировать навыки действия обучаемого в различных нестандартных ситуациях: 1) правильно определить порядок своих действий; 2) грамотно вести переговоры с работниками смежных служб, принимающими участие в устранении неисправности; 3) верно заполнить журнал осмотра формы ДУ-46. В зависимости от принимаемых решений интеллектуальная обучающая система либо переводит пользователя на следующий шаг, либо корректирует его действия, сообщает, что им неправильно сделано и к каким последствиям это может привести в реальной ситуации, направляет к изучению нормативных документов и инструкций [3].

Следует отметить важность для повышения мотивации обучения наличия в информационно-образовательной среде набора мультимедийных ресурсов в поддержку наглядности обучения по ведущим темам специальности 23.02.01 «Организация перевозок и управление на транспорте». Такие ресурсы позволяют ориентироваться в условиях частой смены технологий в профессиональной деятельности по следующим важнейшим темам организации движения поезда, связанным с управлением стрелкой:

– взрез стрелочного перевода.

– потеря контроля стрелочного перевода под проходящим поездом, когда стрелочный перевод поезд уже освободил.

– потеря контроля стрелочного перевода под проходящим поездом, когда поезд не освободил стрелочный перевод.

– потеря контроля стрелочного перевода при отсутствии движения поездов.

– ложная занятость стрелочного изолированного участка.

– перевод стрелки под поездом.

– ложная занятость перегона на участке, оборудованном диспетчерской централизацией, при пассивном дежурстве ДСП (расшифровать) на станциях.

– ложная занятость перегона на участке, оборудованном диспетчерской централизацией, в условиях работы станции без ДСП.

– вспомогательная смена направления движения при диспетчерской централизации района управления Юг.

Для проведения текущего контроля целесообразно использовать тестовые задачи, реализованные в данном программно-техническом комплексе по следующим темам: «Ложная занятость стрелочного изолированного участка» и «Ложная занятость перегона

на участке, оборудованном диспетчерской централизацией». Отчеты по результатам обучения формируются компьютерной системой по каждому обучающемуся, по каждому заданию и по группе в целом.

Был проведен констатирующий эксперимент по выявления направлений повышения эффективности развития компетенций студентов, с использованием как традиционных форм обучения и компьютерного моделирования профессиональной деятельности на компьютере. Полученные данные констатирующего эксперимента показали, что результаты можно разделить на три группы: базовый, повышенный и высокий уровень. Базовый - 45,7 %, Повышенный- 41,7%, Высокий - 13,1%. Результаты обучения убедительны по всем показателям, что может служить основанием для введения соответствующей компетенции – управление движением поездов – в WSR (WorldSkills Russia).

В целях усиления практической составляющей обучения и вхождения WorldSkills Russia в нашем техникуме для оптимального применения информационных технологий обучения изменен график учебного процесса: учебная практика по рабочей профессии приемосдатчика груза и багажа – востребованной на железнодорожных станциях, разделена на две части: выполнение заданий в «бумажной» и компьютерной форме. При такой организации практики бумажные технологии оформления перевозочной документации проходят за одну неделю, а вторая неделя этой практики на втором курсе проводится в учебной лаборатории управления движением с использованием имитационного 3D-тренажера.

Каждый обучающийся получает возможность: подробно изучить конструкцию кузовов вагонов различного типа, их деталей и узлов, реквизитов крепления грузов, типовые схемы погрузки и коммерческие неисправности, получить навыки выполнения коммерческого осмотра различных типов вагонов и оформления его результатов, быстрой и квалифицированной оценки правильности погрузки и крепления разнообразных грузов, устранения выявленных нарушений, обучиться безопасным приемам работы при нахождении на путях станции с точки зрения охраны труда.

Отметим, что информационные технологии позволяют приблизить обучение к реальным действиям при выходе на железнодорожные пути к действующему подвижному составу и при этом исключить травмоопасные ситуации.

Выводы.

Современное программно-технологические оборудование техникума позволяет в условиях цифровой информационной образовательной среды готовить молодого конкурентоспособного профессионала, адаптированного к современным реалиям железной дороги, готового принимать ответственные решения в стандартных и нестандартных ситуациях, в то же время, не подвергая студентов травмоопасности. Возможности высокотехнологичной образовательной среды позволяют коллективу техникума участвовать в государственной программе «Демонстрационный экзамен как форма государственной итоговой аттестации в системе среднего профессионального образования», тем самым обеспечиваю непрерывное повышение квалификации сотрудников.

СПИСОК ЛИТЕРАТУРЫ

1. Виртуальная реальность современного образования: сборник научных статей /сост.: М. Е. Вайндорф-Сысоева, Т.С. Грязнова]. - Москва: МГОУ, 2015. - 91 с.:
2. Официальный сайт WorldSkills Russia https://worldskills.ru/ [Режим доступа 24.09.2018]
3. Трайнев В.А. Новые информационные коммуникационные технологии в образовании /В.А. Трайнев, В.Ю. Теплышев, И.В. Трайнев. – М., 2013. // [Электронный ресурс] – Режим доступа: http://www.iprbookshop.ru/14614.html, свободный. – Загл. с экрана.
4. Сетевая образовательная среда: электронные ресурсы: Учебно-методическое пособие / Под. ред. Т.Н. Носковой. – СПб.: Изд-во РГПУ им. А.И. Герцена, 2015. – 114 с. // [Электронный ресурс] – Режим доступа: https://www.herzen.spb.ru/uploads/ustyugovat/files/, свободный. – Загл. с экрана.

УДК 681.518

ОБ ОСОБЕННОСТЯХ МОДЕЛИ ОЦЕНКИ КАЧЕСТВА СИСТЕМЫ ЭЛЕКТРОННОГО ОБУЧЕНИЯ ПО ISO 9126

Журавлев Антон Евгеньевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mail: zhuravlevae@gumrf.ru

Аннотация. В данной работе осуществлена попытка дополнить стандарт ISO 9126 конкретными характеристиками программного продукта для системы электронного обучения. Это расширение осуществляется путем определения качественных характеристик системы электронного обучения и их интеграции в модель ISO 9126. Результаты представленного исследования послужат основой для оценки существующей системы.

Ключевые слова: модель качества; ISO 9126, ФГОС; электронное обучение.

ABOUT FEATURES OF E-LEARNING SYSTEM QUALITY ASSESSING ACCORDING TO ISO 9126

Zhuravlev Anton
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya Str., St. Petersburg, 198035, Russia
e-mail: zhuravlevae@gumrf.ru

Abstract. This paper made attempt to supplement the ISO 9126 standard with specific characteristics of the software product for the e-learning system. This expansion done by defining the qualitative characteristics of the e-learning system and integrating them into the ISO 9126 model. The results of the presented study will serve as a basis for assessing the existing system.

Keywords: quality model; ISO 9126; GEF; e-learning.

Введение.

Системы организации процесса электронного обучения становятся необходимыми для решения множества реальных задач. Они определяются следующим образом: «метод обучения, использующий ИКТ для полноценной поддержки процесса обучения и аттестации, а также и облегчения процесса приобретения и применения знаний». Экспоненциальный рост ИКТ изменяет систему образования [1], адаптирует ее к современным требованиям и компетенциям, способствует улучшению процесса обучения в целом. Электронное обучение достигает гораздо более широкой целевой аудитории учащихся, которые:

- сильно распределены географически (территориально);
- имеют ограниченные временные и пр. ресурсы;
- могут быть периодически недоступны по различным (например, семейным) обстоятельствам;
- находятся в конфликтных и постконфликтных районах, имеющих проблемы с инфраструктурой;
- имеют трудности при общении в реальном времени (например, при использовании иностранных языков).

Множество подходов и методов обучения при помощи систем электронного и дистанционного обучения уже описаны в соответствующих работах, предоставляющий новый опыт в рамках процесса обучения. Они включают в себя традиционное обучение, электронное обучение, смешанное обучение, мобильное обучение и индивидуальное обучение на основе потребностей учащихся и с использованием моделирования и игр. Было выявлено, что электронное обучение оказывает положительное влияние на успеваемость студентов и производительность преподавательского состава, и все больше организаций внедряют онлайн-обучение и более лояльно относятся к этой концепции обучения. Исследования, проведенные в последние годы, как на Западе, так и РФ, показывают, что, например, в течение 2016-2017 учебного года около 69% государственных и частных школ участвовали в программах финансовой помощи студентам, связанным с курсами дистанционного обучения. Также, например, 81% экономических дисциплин были посвящены онлайн-компоненте.

Кроме того, ряд стран, в том числе и РФ, поощряют развитие систем электронного обучения и оказывают большее давление на учебные заведения в целях обеспечения более гибкого и эффективного обучения. Как указано в работе, электронное обучение является «положительным», если оно своевременно обеспечивает соискателей необходимыми навыками по разумной цене. Многие организации применяют различные подходы и модели для оценки процесса обучения. Вместе с тем высказывалась значительная критика в отношении качества

используемых в настоящее время систем и отсутствия эффективной и универсальной модели оценки качества электронного обучения.

В данной работе уделяется внимание аспекту качества систем электронного обучения, и целью данной работы является исследование основных факторов, способствующих разработке модели качества систем электронного обучения. Модель качества ISO 9126 предложена в качестве основы для оценки систем электронного обучения. Произведена адаптация модели в соответствии со спецификой систем электронного и дистанционного обучения. Адаптация осуществлена путем выделения качественных характеристик веб-систем в целом и систем электронного обучения в частности, и внедрения их в модель оценки качества [2].

На первом этапе работы проведен анализ базового стандарта качества ISO 9126, выявлены его сильные и слабые стороны. Далее предложено первое расширение модели ISO 9126 с качественными характеристиками программного продукта. На следующем этапе выделены и проанализированы основные характеристики веб-систем и систем электронного обучения. На заключительном этапе представлен авторский подход к формированию модели оценки качества, включающий второе расширение модели с характеристиками качества электронного обучения и сделаны выводы о ее применимости и эффективности.

ISO/IEC 9126 представляет собой модель именно качественных характеристик программного обеспечения, потому, наиболее часто она используется для таких этапов жизненного цикла программного обеспечения как:

– обсуждение особенностей, подходов, методик и т.п.;
– планирования проектирования, разработки, тестирования, внедрения, поддержки и т.п.;
– оценка качества готового продукта, его отдельных элементов и пр.

Модель также включает в себя механизмы измерения степени каждой характеристики продукта [3]. Наиболее значимые достоинства модели:

– унифицированность подходов к оценке качества программного обеспечения;
– возможность количественной оценки большинства характеристик;
– простота и доступность механизмов сравнения одного продукта с другим того же класса.
– единое терминологическое пространство.
– широкий охват важнейших аспектов (иерархическая структура, критерии оценки, терминология, простые и точные определения, межуровневые отношения и связи и т.п.);
– расширение возможностей систем поддержки принятия решений, что позволяет избегать дорогостоящих ошибок.

Основные ограничения ISO 9126:

– одним из наиболее важных ограничений модели ISO 9126 является ее обобщенность;
– модель не описывает потребности бизнес-менеджера, которые представлены в факторах рентабельности инвестиций и степени устойчивости
– в модели не представлены механизмы мониторинга программного обеспечения и данных;
– модель не включает в себя методы количественных измерений.

Таким образом, данная модель может использоваться наиболее эффективно при решении следующих задач:

– определение и спецификация требований к качеству программного продукта;
– оценка спецификации программного обеспечения с учетом требований к качеству;
– описание характеристик и атрибутов реализованного программного обеспечения;
– оценка программного обеспечения в период до внедрения;
– оценка программного обеспечения в период до начала эксплуатации.

Из перечисленных ограничений, можно добавить новые характеристики модели оценки качества ISO 9126 для программного продукта [4]. Ниже продемонстрировано одно из расширений модели ISO 9126, описывающее общие и эксплуатационные характеристики, которые способствуют удовлетворению потребностей пользователей различных ролей, а именно:

– конечных пользователей, для которых наиболее востребованным показателем качества является практичность;
– разработчиков программного обеспечения, для которых наиболее значимыми качественными характеристиками программного обеспечения являются надежность и функциональность;
– бизнес-менеджеров, для которых основными факторами качества являются рентабельность инвестиций и устойчивость.

Предлагаемые качественные характеристики программного продукта распределены по трем уровням модели качества:

1) Расширенные характеристики первого уровня.

– Отслеживаемость – используется для мониторинга внутренних процессов, происходящих в ходе функционирования программного обеспечения;
– Согласованность (данные) – определяет степень согласованности данных программного обеспечения между собой;
– Рентабельность – показатель, определяющий экономическую эффективность проекта т.е. рентабельность инвестиций как один из основных аспектов деятельности бизнес-менеджера;
– Устойчивость – показатель, также являющийся важным критерия менеджмента и определяющий степень устойчивости программного обеспечения к воздействиям внешней среды;

2) Расширенные характеристики второго уровня

– Управляемость – комплексная характеристика, определяющая легкость, скорость, эффективность и простоту доступа пользователей к контенту;

– Поддерживаемость – характеристика, определяющая пользовательскую практичность.

3) Расширенные характеристики третьего уровня

– Осмысленность – параметр, часть характеристики «Пригодность», определяющая когнитивную нагрузка на пользователя;

– Простота – параметр, определяющий требования к уровню вхождения пользователя, часть характеристики «Привлекательность»;

– Цветность – параметр, определяющий палитру и внешнюю восприимчивость дизайна, часть характеристики «Привлекательность»;

– Читабельность – параметр, определяющий общую понятность контента, часть характеристики «Привлекательность».

Необходимо отметить, что ISO 9126 сравнивался с другими моделями оценки качества (MaCall, FURP и Dromey). Стало очевидно, что основное достоинство выбранной модели заключается в том, что она универсальна и может использоваться во многих видах систем, сфер и отраслей, включая академическую область, т.е. системы электронного и дистанционного обучения. Стандарт ISO 9126 был использован для оценки систем электронного обучения среди учителей, профессорско-преподавательского состава и администрации учебных заведений среднего и, средне-специального и высшего профессионального образования. Благодаря этому были выбраны и сформулированы универсальные внешние системы оценки качественных характеристик и параметров для эксплуатационных, административных, электронных, технологических, управленческих и экономических факторов в системах электронного обучения, а также сформулированы определяющие критерии оценки B2B приложений.

Можно сделать вывод о том, что стандарт ISO 9126 подходит для использования при оценке систем электронного обучения, поскольку он широко используется в сообществе разработчиков программного обеспечения, адаптирован к различным областям и контекстам и прост в использовании и понимании его пользователями. В следующем разделе представлен подход к качеству, основанный на адаптации модели оценки качества ISO к системам электронного обучения.

Авторский подход к оценке качества. Для достижения успеха в современном бурно развивающемся секторе оказания образовательных услуг образовательные организации нуждаются в высоком качестве приложений электронного обучения [5]. Предлагаемый подход к оценке качества организован в два этапа:

1) определение дополнительных характеристик, характерных для систем электронного обучения;

2) добавление этих характеристик в общую модель оценки качества ISO 9126.

Определение характеристик систем электронного обучения для общего стандарта ISO 9126 означает, что для его полной адаптации к электронному обучению необходим дальнейший анализ и расширение характеристик. Из определений термина «электронное обучение» становятся понятны акценты на способ получения информации, т.е. на приобретение и использование знаний, которые распространяются и облегчаются главным образом с помощью электронных средств. Такие электронные средства могут включать в себя интернет, интранет, экстранет и различные мультимедиа технологии, что в значительной мере определяет факторы, от которых зависит качество систем электронного обучения:

– качество веб-технологий;

– качество содержания обучения и используемых педагогических и познавательных подходов;

– рентабельность инвестиций и устойчивость программного обеспечения для электронного обучения (характеристики качества бизнеса)

В исследовании обобщены качественные характеристики веб-приложений (см. табл. 1) и определены четыре основных качественных характеристики B2B-приложений:

– отслеживаемость;

– доступность;

– управляемость;

– настраиваемость.

Исходя из этого, характеристики оценки качества для систем электронного обучения были определены следующим образом:

– Отслеживаемость – используется для отслеживания процесса электронного обучения, таких как создание, формирование и передача учебного контента;

– Понятность – определяет степень доступности учебного контента для понимания учащихся. Понятность имеет большое значение в приложениях электронного обучения;

– Управляемость – комплексная характеристика, определяющая легкость, скорость, эффективность и простоту доступа пользователей к контенту;

– Доступность – способность системы электронного обучения обеспечить доступ для удаленных мест.

Качество учебного контента и используемых педагогических и когнитивных подходов, а, следовательно, и качество электронного учебного курса в целом повышается за счет следующих факторов:

– Контент, ориентированный на учащегося – относится к возможностям программного обеспечения для электронного обучения в соответствии с потребностями, ролями и обязанностями учащихся. Программное

обеспечение для электронного обучения должно обеспечивать подачу знаний, наработку и тестирование навыков, а также осуществлять информационную поддержку своих учащихся;

– Фрагментарность (гранулярность) – определяет возможность и степень сегментации учебного контента, что логично структурирует и облегчает усвоение новых знаний, а также позволяет гибкое планирование учебного времени;

– Привлекательный контент – является основным мотивирующим фактором программного обеспечения электронного обучения. Обучающие модели и методы должны использоваться для разработки привлекательного контента;

– Интерактивность – обеспечивает поддержку и акцентирование внимание обучающегося как на определенные элементы контента, так и к программному обеспечению электронного обучения в целом. Для содействия обучению используется интенсификация взаимодействия учащихся с системой и между собой;

– Персонализация – реализует возможность программного обеспечения электронного обучения индивидуально подстраивается под требования, интересы и потребности учащихся;

– Согласованность (данные) – обеспечивает взаимную согласованность данных контента программного обеспечения электронного обучения;

– Коммуникация и совместное обучение – наделяет программное обеспечение электронного обучения гибкими средствами коммуникации, обмена, сотрудничества и развития не только базовых навыков ИКТ, но и всего спектра социальных и коммуникационных навыков;

– Быстрое распределение учебных материалов – предоставляет открытый подход к материалам и наиболее быстрое распределение учебного контента.

Крайне важными остаются качественные бизнес-характеристики, т.е. параметры системы, напрямую связанные с экономическими факторами. Например, показатель окупаемости, т.е. отдачи от инвестиций имеет большое значение для организаций, предоставляющих системы электронного обучения; его можно измерить с помощью:

– реакции обучающегося в конце курса;
– отношения к изменениям в ходе учебного процесса;
– улучшения знаний и навыков обучающегося;
– изменения поведения обучающегося;
– результатов изменений в сфере деятельности обучающегося.

Также, например, устойчивость определяет степень, собственно, устойчивости программного обеспечения электронного обучения на рынке с точки зрения бизнес-менеджеров. В таблице 2 перечислены наиболее важные качественные характеристики систем электронного обучения.

После определения качественных характеристики системы электронного обучения, они интегрируются в общую модель качества. Также покажем интеграцию этих характеристик на втором уровне модели.

Интеграция в характеристику «Надежность»:

– Доступность.

Интеграция в характеристику «Функциональность»:

– Понятность;
– Ориентированность;
– Детализируемость;
– Привлекательность;
– Интерактивность;
– Персонализированность;
– Коммуникативность;

Интеграция в характеристику «Эффективность»:

– Распространяемость.

Заключение.

В данной работе предложена модель оценки качества программных продуктов в электронном обучении на основе стандарта ISO 9126. Непосредственный вклад этой работы связан с выявлением новых качественных характеристик систем электронного обучения. Будущие исследования в этой области включают в себя проверку и оценку предлагаемой модели на практике, на базе коммерческой образовательной организации и государственного университета, а также и разработку инструмента автоматизированной оценки качества систем электронного обучения на основе ISO 9126.

СПИСОК ЛИТЕРАТУРЫ

1. Крупенина Н. В. Организация распределенной системы подготовки и проведения электронного тестирования для оценки соответствия профессиональных компетенций работников морских специальностей / Н. В. Крупенина, Н. Ю. Барышникова, Л. Н. Тындыкарь // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2015. — № 3 (31). — С. 216–228.
2. Бобыр Е. И. Комплексная модель адаптивной компьютеризированной системы обучения и тестирования на базе семантических сетей / Е. И. Бобыр, Л. Н. Радванская, В. В. Мартынов, Ю. В. Чепурная // Вестник Херсонского национального технического университета. — 2009. — № 1 (34). — С. 491–496.
3. Журавлев А.Е. Автоматизация системы оценки качества освоения учебной программы / А. Е. Журавлев // Матер. XXV межд. конф. «Применение новых технологий в образовании», «ИТО-Троицк-2014». — М.: БАЙТИК, 2014. — С. 412–413.
4. Журавлев А.Е. Разработка и внедрение интегрируемой программно-аппаратной системы тренинга и аттестации на примере

транспортного ВУЗа / Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — СПб.: ГУМРФ имени адмирала С. О. Макарова, 2016. — Вып. 6 (40). — 260 с. Стр. 242-251.
5. Журавлев А.Е. Внедрение тестовой системы на базе решения «1С:Экзаменатор» и ее адаптация к актуальным ФГОС / Новые информационные технологии в образовании: Сборник научных трудов 17-й международной научно-практической конференции «Новые информационные технологии в образовании» (Инновации в экономике и образовании на базе технологических решений «1С») 31 января–1 февраля 2017 г. /Под общ. ред. проф. Д.В. Чистова. Часть 2.– М.: ООО «1С-Паблишинг», 2017. 389 с.: илл. Стр. 75-78.

УДК 303.732(075)

ТЕОРИЯ СИСТЕМНЫХ ИССЛЕДОВАНИЙ КАК ОСНОВА ФУНДАМЕНТАЛЬНОЙ ОБЩЕНАУЧНОЙ ПОДГОТОВКИ МОЛОДЫХ УЧЕНЫХ

Калинин Владимир Николаевич
Военно-космическая академия имени А.Ф.Можайского
Ждановская ул., 13, Санкт-Петербург, 197198, Россия
e-mail: kvn.112@mail.ru

Аннотация. В статье рассматривается научно-педагогическая концепция системно-кибернетической подготовки молодых ученых на третьей ступени высшего образования (аспирантура), отражающая многолетний опыт подготовки и современное состояние и тенденции развития теоретико-системных исследований. Излагаются целевая установка, дидактические задачи и структура соответствующей учебной дисциплины «Теоретические основы системных исследований».

Ключевые слова: теория системных исследований; динамическая система по Калману; кибернетика по Бергу, математическая структура; системно-кибернетическая подготовка.

THE THEORY OF SYSTEM RESEARCHES AS A BASIS OF FUNDAMENTAL GENERAL SCIENTIFIC PREPARATION OF YOUNG SCIENTISTS

Kalinin Vladimir
Military space academy named A.F. Mozhayskogo
13 Zhdanovskaya Str., St. Petersburg, 197198, Russia
e-mail: kvn.112@mail.ru

Abstract. In article the scientific and pedagogical concept of system-cybernetic preparation of young scientists at the third step of higher education (postgraduate study) reflecting long-term experience of preparation and a current state and tendencies of development of system researches is considered. The purpose, didactic problems and structure of a corresponding subject matter «Theoretical bases of system researches» are stated.

Keywords: the theory of system researches; Kalmans dynamic system; Bergs cybernetics; mathematical structure; system-cybernetic preparation.

Введение.

Анализ многолетнего опыта научных исследований показывает, что при их проведении авторы придерживаются следующих двух концепций.

Первая из них, которая может быть названа индуктивным подходом (от частного – к более общему), заключается в том, что новое научное знание формируется как развитие уже известного решения частной научной задачи – как расширение и модификация (порой весьма незначительная) известных частных результатов. Именно так (от частного результата – к расширенному частному и весьма редко – к широкому обобщению) организуется работа многих научных школ, группирующихся вокруг научного руководителя.

При этом могут быть получены весьма ценные результаты, однако главный недостаток индуктивного подхода заключается в том, что его использование зачастую приводит к изоляционизму, дифференциации и увеличению энтропии знаний и тезауруса. Кроме того, соответствующие исследования неизбежно оказываются ограниченными рамками принятой в данной научной школе методологии. Все это затрудняет обобщение результатов, обмен опытом научных исследований и подготовку специалистов широкого профиля. Этот путь хорош для начинающих ученых, но иногда может приводить в тупик. По этому поводу американский экономист Кеннет Боулдинг как-то заметил, что индуктивный путь развития науки может привести к тому, что ученое сообщество превратится «в сборище замуровавшихся поодиночке отшельников, каждый из которых бормочет про себя слова на языке, понятном только ему одному» [1].

Вторая, альтернативная и более продуктивная концепция – дедуктивный подход (от общего – к частному). Этот подход реализуется тогда, когда исследователь, обладающий фундаментальной подготовкой в достаточно общей области, «проецирует» изучаемую частную задачу на проблематику более широкой науки, интерпретируя эту задачу в обобщающих терминах и используя для ее решения соответствующую более общую методологию с последующим возвращением в прикладную область и интерпретацией полученных результатов в соответствующих специальных терминах и представлениях. Именно на этом пути можно ожидать новых и крупных научных достижений.

Ярким примером дедуктивного подхода является использование системно-кибернетической методологии, носящей универсальный характер. Получаемые при этом результаты отличаются высокой

степенью общности и позволяют обеспечить взаимопонимание и обмен опытом между специалистами различного узкого профиля. Остановимся на этом вопросе более подробно.

1. Тенденция интеграции научных знаний и формирование системно-кибернетических представлений. Системно-кибернетическая методология как одна из трех основ прикладных научных исследований.

По мере накопления знаний и расширения сферы научных исследований, обусловленного требованиями общественной практики, начиная с XVIII века, в развитии науки все более отчетливо стала проявляться тенденция дифференциации знаний, выражающаяся в увеличении количества отдельных наук и в ослаблении связей между ними.

Поэтому одновременно с процессом дифференциации знаний, в общенаучной методологии возникла тенденция интеграции знаний, примером которой явилось формирование в XX веке нового научного направления, основу которого составили такие фундаментальные обобщающие понятия и концепции, как система, среда, концепция системного подхода. Развитие соответствующих системных представлений во второй половине XX века привело к формированию фундаментального понятия динамической системы по Калману (как математического отражения принципа причинности) и соответствующей концепции кибернетического подхода к исследованию реальных объектов материальной культуры, основанного на рассмотрении этих объектов как динамических систем, «погруженных» в управляющую и возмущающую среды (рис.1).

Важную роль при этом сыграло введенное академиком А. Бергом определение кибернетики как «науки об оптимальном управлении сложными динамическими системами». Он называл кибернетику «наукой величайших возможностей». С математической точки зрения основополагающую роль здесь сыграла теория математических структур по Н. Бурбаки, которая позволяет адекватно и конструктивно формализовать соответствующие системные и системно-кибернетические представления.

Рис.1. Объект системно-кибернетических исследований

Системное направление интеграции знаний в современной науке позволило с единых позиций объединить проблематику и методологию частных интегральных наук (таких, как исследование операций, теория игр, теория принятия решений и др.) на основе тезауруса, концепций и математических конструкций триады фундаментальных источников:

– общей теории систем – понятия системы и среды, концепция системного подхода;

– кибернетики по акад. А.И. Бергу – понятия динамической системы, управляющей и возмущающей среды, оптимального выбора управляющего воздействия;

– теории математических структур Н. Бурбаки – концепция и математическое определение математической структуры, которая в данном случае может рассматриваться как наиболее общая формальная модель системы и среды, а также математическая конструкция, лежащая в основе постановки задач системного исследования.

Соответствующие системные взгляды удивительным образом оказались гармонично согласованными с бурным развитием в послевоенный период математического инструментария, связанного с исследованием сложных математических задач оптимального выбора, не поддающихся классическим методам решения. Особо важную роль здесь сыграли работы акад. Л.С. Понтрягина (принцип максимума), Р. Беллмана (принцип оптимальности) и др.

Все это позволяет говорить о становлении во второй половине XX века нового фундаментального направления в современной науке, которое может быть названо теорией системных (точнее, системно-кибернетических) исследований.

Исходя из приведенных взглядов и положений, уточним предмет системных исследований.

Предметом теории системных (системно-кибернетических) исследований является изучение структуры и общих закономерностей функционирования систем любой материальной природы, общих свойств этих систем и разработка методов управления ими на основе соответствующих концептуальных и математических моделей.

Это фундаментальное направление занимает важное место в современной науке. Если раньше прикладные (в том числе технические) науки базировались на двух основах – фундаментальных (естественных и гуманитарных) науках и математике, то теперь к ним предлагается добавить, в качестве третьей основы (третьего «кита»), системно-кибернетическую методологию. При этом в качестве общеметодологической

основы сохраняется философское знание и понимание как универсальная система наиболее общих мировоззренческих взглядов.

2. Научно-педагогическая концепция системно-кибернетической подготовки. Базовая учебная дисциплина для адъюнктов (аспирантов) «Теоретические основы системных исследований» – целевая установка, структура и краткое содержание

В соответствии с вышеизложенным можно утверждать, что указанная теория должна занять важное место в подготовке современных молодых ученых. По мнению автора, излагаемые в рамках этой теории системные представления, методологические концепции и принципы помогут исследователю уверенно ориентироваться в современном «океане» различных частных подходов и методов исследования конкретных систем, увидеть общее в этих подходах и методах, и могут явиться конструктивной основой постановки и решения новых прикладных научных задач, связанных с исследованием реальных сложных динамических систем любой физической природы и оптимальным управлением этими системами в условиях различных возмущающих воздействий. Отсюда следует необходимость коррекции существующей системы подготовки молодых ученых.

Соответствующая научно-педагогическая система, которая была названа системно-кибернетической подготовкой, была разработана и внедрена в образовательный процесс в Военно-космической академии имени А.Ф. Можайского в 70-е годы прошлого века [2], успешно апробирована в течение нескольких десятилетий и нашла отражение в ряде учебников и учебных пособий [3–7]. В последние годы указанный подход нашел отражение в учебной дисциплине «Теоретические основы системных исследований», которая читается всем адъюнктам академии. Рассмотрим краткую характеристику этой дисциплины.

Целью рассматриваемой учебной дисциплины является формирование у обучающихся следующих компетенций. Адъюнкт (аспирант) должен быть способен:

– выявить системную сущность исследуемой прикладной научной задачи и осуществить ее вербальную и математическую постановку на основе системно-кибернетических представлений;

– осуществить обоснованный выбор метода решения научной задачи в рамках современной системно-кибернетической методологии и практическое получение решений с последующей их интерпретацией в рассматриваемой предметной области.

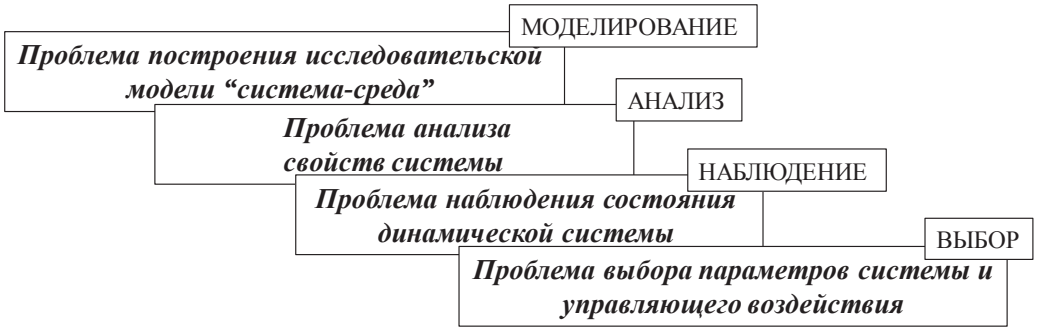


Рис.2. Проблемы системно-кибернетических исследований

Для достижения указанной выше цели необходимо решение следующих трех дидактических задач:

– формирование у обучающихся навыков системного мышления, системно-кибернетической трактовки закономерностей функционирования сложных технических и организационно-технических систем;

– изучение принципов вербальной и математической постановки и решения четырех основных проблем системного исследования – проблемы моделирования системы и среды, проблемы анализа свойств системы, проблемы наблюдения состояния (применительно к динамическим системам) и проблемы выбора (структурных параметров системы или управляющего воздействия) применительно к различным типам возмущающей среды (рис.4, 5) (более подробно см. [3, 8]);

– изучение основных понятий и методов системного анализа как инструмента исследования сложных систем в условиях существенной неопределенности на основе сбора и обработки экспертной информации.

Структурно учебный материал сгруппирован вокруг четырех указанных выше фундаментальных проблем системных исследований (моделирование – анализ – наблюдение – выбор) и изложен в семнадцати темах, объединенных в следующие шесть образовательных модулей (разделов).

Раздел первый. Общая характеристика системно-кибернетических исследований – модуль №1 «ОБЩИЙ».

1. Краткий исторический очерк и тенденции в развитии научных знаний. Предмет системных (системно-кибернетических) исследований.

2. Основные системно-кибернетические понятия. Сущность системного подхода. Система, среда и время. Понятие о динамической системе.

3. Четыре фундаментальные проблемы системно-кибернетических исследований.

Раздел второй. Математическое моделирование систем – модуль №2 «МОДЕЛЬ».

4. Основные математические конструкции в моделировании систем.
5. Математические модели статических систем.
6. Математические модели динамических систем.

Раздел третий. Анализ свойств систем – модуль №3 «АНАЛИЗ».

7. Проблема анализа свойств статических систем.
8. Проблема анализа свойств динамических систем.

Раздел четвертый. Проблема наблюдения состояния динамической системы – модуль №4 «НАБЛЮДЕНИЕ».

9. Общая постановка проблемы наблюдения состояния динамической системы и идеальные алгоритмы наблюдения.
10. Алгоритмы наблюдения состояния динамической системы в условиях стохастической среды.

Раздел пятый. Проблема выбора в системно-кибернетических исследованиях – модуль №5 «ВЫБОР»

11. Общая характеристика и математическая постановка проблемы выбора.
12. Оптимальный выбор структурных характеристик (параметров) системы.
13. Проблема оптимального управления динамической системой и основные принципы ее решения.
14. Основные принципы однокритериального выбора в условиях неопределенности.
15. Проблема многокритериального выбора и основные принципы ее решения.

Раздел шестой. Основные понятия и методы системного анализа – модуль №6 «СИСТЕМНЫЙ АНАЛИЗ».

16. Основные понятия, проблемы и общие принципы системного анализа.
17. Основные понятия и методы научно-технического прогнозирования.

Изучение дисциплины целесообразно организовать во втором семестре обучения. Ее объем, по мнению автора, ориентировочно должен составлять от 4 (программа-минимум) до 6 (программа-максимум) зачетных единиц. Для программы-максимум этот объем включает: лекций – 80 часов, семинаров – 24 часа, экзамен. В 2016 году издан учебник «Теоретические основы системных исследований» [3], содержащий программу дисциплины и необходимое учебно-методическое обеспечение соответствующего учебного процесса.

Более подробно опыт системно-кибернетической подготовки на основе курса «Теоретические основы системных исследований» с учетом особенностей специальностей подготовки изложен в статье [9].

Заключение.

Многолетний опыт системно-кибернетической подготовки адъюнктов Военно-космической академии имени А.Ф. Можайского, основанный на вышеизложенных принципах, показал, что изучение рассмотренной учебной дисциплины и овладение системными представлениями и соответствующими методологическими концепциями позволяет существенно расширить кругозор начинающего молодого исследователя.

Теоретико-системные знания помогают ему уверенно ориентироваться в современном изобилии различных частных подходов и методов исследования сложных конкретных военно-технических систем, увидеть общее в этих подходах и методах, являются конструктивной основой постановки и решения новых прикладных научных задач, связанных с исследованием реальных сложных динамических систем любой физической природы, наблюдением их состояния и оптимальным управлением этими системами в условиях различных возмущающих воздействий.

Все это позволяет вооружить молодых ученых новейшими методами исследования сложных систем, значительно повысить уровень выполняемых ими научно-исследовательских (диссертационных) работ. Автор надеется, что изложенная в статье научно-педагогическая концепция подготовки молодых ученых окажется полезной в образовательном процессе военных вузов и научно-исследовательских организаций.

СПИСОК ЛИТЕРАТУРЫ

1. Kenneth Boulding. General Systems Theory - the Skeleton of Science // General Systems, 1956, vol. I, pp. 11–17.
2. Калинин В.Н., Резников Б.А. Теория систем и управления (структурно-математический подход): учебное пособие. – Л.: ВИКИ им. А.Ф. Можайского, 1978. – 418 с.
3. Калинин В.Н. Теоретические основы системных исследований: учебник для адъюнктов/ – СПб.: ВКА им. А.Ф. Можайского, 2016. – 293 с.
4. Калинин В.Н., Резников Б.А., Варакин Е.И. Теория систем и оптимального управления: учебник. – Л.: ВИКИ им. А.Ф. Можайского, 1979, 1989. – Ч. I: Основные понятия, математические модели и методы анализа систем. – 319 с.; – МО СССР, 1987. – Ч. II: Понятия, модели, методы и алгоритмы оптимального выбора. – 589 с.
5. Москвин Б.В. Теория принятия решений: учебник. – СПб.: ВКА им. А.Ф. Можайского, 2005. – 384 с.
6. Резников Б.А. Системный анализ и методы системотехники: учебник. – МО СССР, 1990. – Ч. I: Методология системных исследований. Моделирование сложных систем. – 522 с.
7. Военная системотехника и системный анализ: учебник. – МО СССР, 1999. Ч. II: Модели и методы подготовки и принятия решений в сложных организационно-технических комплексах в условиях неопределенности и многокритериальности / под ред. проф. Соколова Б.В. – 496 с.
8. Калинин В.Н. Морфологический анализ проблематики системных исследований // Труды СПИИРАН. – 2013. Вып. 1(24). – С. 89–107.
9. Калинин В.Н., Соколов Б.В. Теория системных исследований как основа фундаментальной общенаучной подготовки молодых ученых // Стратегические приоритеты. –2017. № 2. – С. 127–130.

УДК 378.14

АНАЛИЗ ПРИМЕНЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ «ГАЛАКТИКА ERP» В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ

Локнов Алексей Игоревич, Примакин Алексей Иванович
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: info_for_aleksey@mail.ru, a.primakin@mail.ru

Аннотация. В статье проведён анализ применения автоматизированной системы управления «Галактика ERP» в Санкт-Петербургском университете МВД России. Рассмотрены результаты её внедрения в организацию образовательного процесса. Сформулированы предложения по дальнейшему использованию и полноценному функционированию системы «Галактика ERP» при выполнении ежедневных задач.

Ключевые слова: образовательный процесс; инновации в образовании; автоматизированная система управления в образовательном процессе.

ANALYSIS OF THE USE OF THE AUTOMATED CONTROL SYSTEM «GALAXY ERP» IN THE EDUCATIONAL PROCESS OF ST. PETERSBURG UNIVERSITY OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Loknov Aleksey, Primakin Alexey
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mails: info_for_aleksey@mail.ru, a.primakin@mail.ru

Abstract. In the article the analysis of application of the automated control system «Galaktika ERP» in Saint-Petersburg University of MIA of Russia. The results of its implementation in the organization of educational process are considered. The proposals for the further use and full functioning of the Galaxy ERP system in performing daily tasks are formulated.

Keywords: educational process; innovations in education; automated control system in the educational process.

Федеральные государственные образовательные стандарты высшего образования устанавливают высокие требования к содержанию электронной образовательной среды. Среди них обеспечение доступа к основополагающим документам, регламентирующим получение знаний, постоянная фиксация хода образования, применение дистанционных образовательных технологий, взаимодействие между участниками образовательного процесса и многие другие. Для успешного функционирования всех элементов системы необходимы современные средства информационно-коммуникационных технологий [1-7]. Одним из способов обеспечения работы является использование автоматизированной системы в управлении образовательной организацией высшего образования.

Руководством Санкт-Петербургского университета МВД России в конце 2016 года было принято решение о заключении государственного контракта с корпорацией «Галактика» на установку разработанных ею программных продуктов для автоматизации образовательной деятельности.

«Галактика» – российская компания, которая разрабатывает и предоставляет продукты в информационной сфере более 30 лет. Все эти годы идёт непрерывный процесс совершенствования товаров и услуг. Наряду со многими отраслями, где используются базовый программный продукт корпорации – система «Галактика ERP», разработано и специализированное решение для сферы образования. Оно реализовано в комплексе «Галактика Управление Вузом» и в Системе Галактика «Расписание учебных занятий». В настоящее время уже более 50 образовательных организаций высшего образования страны используют эти программные продукты [8].

Для построения эффективной системы управления структурой образовательной организации и оптимизации учебного процесса Санкт-Петербургским университетом МВД России закуплен и успешно используется ряд модулей системы «Галактика ERP» в рамках решения «Галактика Управление Вузом», среди них:

- управление персоналом;
- приёмная кампания;
- управление контингентом обучающихся;
- учебный процесс;
- учёт успеваемости;
- обмен бизнес-документами;
- рабочее место пользователя;
- настройка.

Модуль «управление персоналом» – предназначен для организации ведения штатного расписания и планирования фонда оплаты труда в образовательной организации высшего образования. «Приёмная кампания» - используется для решения задач по планированию и организации вступительных испытаний, построения рейтинговых списков, ведения личных дел абитуриентов, выгрузки в федеральные информационные системы.

Модули «управление контингентом студентов», «учебный процесс», «учёт успеваемости» являются основными для полноценной автоматизации образовательной деятельности. Модуль «управление контингентом студентов» позволяет вести личные дела обучающихся и формировать реестр приказов со всеми необходимыми видами распорядительных действий. Информация представлена в виде личной карточки обучающегося и сгруппирована в 12 разделах (Общие сведения, учебная карточка, Награждения, Родственники, Предыдущее образование, Воинский учет и др.). Модуль «учебный процесс» предназначен для ведения учебных планов, расчёта нагрузки кафедр и научно-педагогических работников. Модуль «учёт успеваемости студентов» используется для формирования зачётных и экзаменационных ведомостей, ведения баз данных выпускных квалификационных и курсовых работ, печати дипломов и приложений к ним, анализа успеваемости в различных разрезах. Модули «обмен бизнес-документами», «рабочее место пользователя», «настройка» применяются в большей степени для организации информационного обмена, обеспечения безопасности эксплуатации системы «Галактика ERP», поддержки пользователей. В рамках администрирования системы выполняются мероприятия, направленные на сохранность базы данных при эксплуатации, поддержание целостности и непротиворечивости информации.

«Расписание учебных занятий» – отдельная система, на новой платформе интегрированная с системой «Галактика Управление Вузом». Её появление связано с большим количеством новых сложных задач для удовлетворения современных потребностей в информационной сфере. Она решает одну из ключевых задач образовательной организации высшего образования – планирование и построение расписания занятий в образовательной организации, получение всех возможных видов отчетности и обеспечение удобного сервиса для преподавателей и студентов (курсантов, слушателей).

Изначально был разработан план-график проекта внедрения системы автоматизации образовательного процесса «Галактика ERP». В нём обозначены основные мероприятия по внедрению, установлены даты начала и окончания работ, сроки реализации, определены ответственности заказчика и исполнителя. В университете сформированы пять рабочих групп по основным установленным модулям:

- приёмная комиссия;
- управление контингентом обучающихся;
- учебный процесс;
- учёт успеваемости обучающихся;
- расписание учебных занятий.

Каждая учебная группа состояла из руководителя и сотрудников в служебные обязанности, которых входит непосредственно исполнение функций по специализации направленности группы. Общее руководство работой возложено на начальника управления учебно-методической работы. На начальном этапе была произведена установка системы «Галактика ERP». Сформированы общесистемные каталоги, содержащие исходную информацию. Для работы в программе введены так называемые СЕРШ – структурные единицы штатного расписания, основополагающие элементы, формирующие организационно-штатную структуру университета.

Первое применение системы «Галактика ERP» в управлении образовательным процессом произошло во время мероприятий по набору на обучение. Модуль «приёмная кампания» использовался в июле 2017 года при приёме абитуриентов в университет на очную форму обучения и в сентябре 2017 года при наборе слушателей на заочную форму обучения. Он получил положительные отзывы. Среди них уменьшение количества затрачиваемого времени на работу, избежание ошибок «человеческого фактора», оптимизирование и исключение «двойной» работы в повседневной деятельности, создание условий для перераспределения служебных обязанностей. Это достигается за счёт возможности экономии времени при импортировании данных из ФИС ЕГЭ (быстрая проверка результатов единого государственного экзамена) и при экспортировании данных о вступительных испытаниях в федеральную информационную систему. За счёт формирования электронных учебных дел данные о поступивших абитуриентах после зачисления автоматически передаются на факультет. А о кандидатах, не прошедших отбор формируется электронный архив.

Для полноценного использования остальных модулей, в рамках образовательного процесса, была поставлена задача по введению всей основополагающей информации. Первым был осуществлён ввод учебных планов на каждый год приёма по очной форме обучения в модуле «Учебный процесс». Для этого произведено закрепление всех преподаваемых в университете дисциплин за кафедрами с учётом последних организационно-штатных мероприятий. Наполнены содержания каждой дисциплины (виды занятий, количество учебных часов, трудоёмкость, последовательность прохождения) и введены в перечень дисциплин плана. Сформированы календарные учебные графики. Всего занесено в систему более 100 учебных планов. Практика использования показывает, что, имея перед собой во время работы доступ к любому учебному плану в электронном виде, создаётся возможность быстрого выполнения поставленной задачи.

За период использования системы «Галактика ERP» университетом, с представителями корпорации «Галактика» было организовано и проведено двенадцать рабочих совещаний, на которых были получены консультации и сформирована общая координация действий по внедрению программы. Двое сотрудников Санкт-Петербургского университета МВД России прошли обучение работе в системе.

В ходе многочисленных вэбинаров, проводимых представителями компании «Галактика», были получены знания, как данные по переменному составу университета на основании специальным образом предварительно заполненных таблиц загрузить в систему «Галактика ERP». Для этого используется специальный редактор дающий возможность импортировать файлы из формата Excel и переводить их в формат DBF. При его помощи

таблицы вводятся в систему через импортирование. Успешный опыт этой загрузки позволяет действовать автономно в данном вопросе без представителей компании «Галактика» и при необходимости самостоятельно перезагружать информацию об обучающихся. В соответствии с план-графиком проекта внедрения системы автоматизации образовательного процесса «Галактика ERP» внесены данные по пяти факультетам.

Зачисленные для обучения курсанты-первокурсники распределяются по группам и по узким специализациям при помощи системы приказов, предусмотренной в «Галактике ERP». Для создания, которых были сформированы справочники распорядительных действий по студентам. Приказы используются для всех предпринимаемых действий по обучающимся в рамках образовательного процесса (перевод, назначения и т.д.). В модуле «управление контингентом студентов» содержится «реестр приказов по студентам» хранящий историй всех приказов, проводимых в системе. По работе в данном модуле были проведены ряд занятий со старшими инспекторами учебной части факультетов.

На текущий момент проводится работа по подготовке к составлению расписания учебных занятий в системе «Галактика ERP». Для этого произведена загрузка аудиторного фонда в систему и внесены данные по научно-педагогическим работникам университета. Осуществлена демонстрация системы расписания и проведён ряд занятий с сотрудниками управления учебно-методической работы задействованных в планировании образовательного процесса, что позволило начать работу в Системе Галактика «Расписание учебных занятий» по заполнению сетки пар, академических календарей, справочников. Назначить виды работ, заполнить содержание нагрузок. В рамках администрирования проводится работа по корректировке постоянного состава и аудиторий для учёбы. Выполняется репликация данных, конфигурирование меню и окон для соответствующих пользователей, и их техническая поддержка, совершается постоянный мониторинг работы. Готовятся предложения по модернизации подсчёта рейтинговых данных деятельности научно-педагогических работников [9] в рамках модуля «обмен бизнес-документами». Рассматривается возможность введения электронного дневника обучающегося.

На сегодняшний день для полноценного функционирования «Галактики» стоит ряд задач, поставленных руководством университета. Среди них первая – разработка расписания в электронном виде. Планируется наряду с учебным расписанием, составленным «вручную», параллельно вводить расписание, составленное в «Галактике». Вторая – создание локального нормативно-правового акта, регламентирующего размещение информации в системе «Галактика ERP». Необходимо обозначить подразделения, отвечающие за вводимые данные, ответственных лиц, их руководителей. В качестве альтернативы рассматривается вариант создания приложения к приказу об организации образовательной деятельности на учебный год. Поскольку этот приказ ежегодно обновляется, информация об ответственных лицах будет всегда актуальна, так как происходит естественная ротация сотрудников, а данные всегда остаются за подразделениями. Третья – организовать информирование среди личного состава о системе «Галактика ERP». Предусматривается выступления на различных совещаниях о ходе внедрения «Галактики». Планируется издание информационных пособий и передача их в подразделения. Четвёртая – администрирование системы. В «Галактике» нужно чётко разграничить права и зоны ответственности. Необходимо исключить случаи изменения основополагающих данных по образовательному процессу сторонними подразделениями. В случае появления нового положительного опыта своевременно доводить до сведения заинтересованных лиц.

Таким образом, применение системы «Галактика ERP» даёт возможность производить естественный, органичный обмен данными между подразделениями университета. Позволяет систематизировать возникающие информационные потоки, требующие контроля и чёткого перераспределения. Допускает получение информации об образовательном процессе в режиме реального времени.

СПИСОК ЛИТЕРАТУРЫ

1. Об образовании в Российской Федерации: Федеральный закон от 29.12.2012 г. № 273-ФЗ.
2. Приказ Министерства образования и науки РФ от 1 декабря 2016 г. № 1511 «Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 40.03.01 Юриспруденция (уровень бакалавриата)».
3. Приказ Министерства образования и науки РФ от 19 декабря 2016 г. № 1614 «Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 40.05.01 Правовое обеспечение национальной безопасности (уровень специалитета)».
4. Приказ Министерства образования и науки РФ от 16 ноября 2016 г. № 1424 «Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 40.05.02 Правоохранительная деятельность (уровень специалитета)».
5. Приказ Министерства образования и науки РФ от 28 октября 2016 г. № 1342 «Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 40.05.03 Судебная экспертиза (уровень специалитета)».
6. Приказ Министерства образования и науки РФ от 16 января 2017 г. № 20 «Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 38.05.01 Экономическая безопасность (уровень специалитета)».
7. Приказ Министерства образования и науки РФ от 19 декабря 2016 г. № 1612 «Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере (уровень специалитета)».
8. Официальный сайт Корпорации «Галактика».
9. Кустов П.В., Локнов А.И. Качество мониторинга деятельности научно-педагогических работников как эффективное средство повышения качества образовательного процесса // Вестник Санкт-Петербургского университета МВД России. 2017. № 3 (75). С. 168 – 171.

УДК 681.5.03

ИННОВАЦИОННЫЕ МЕТОДЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Парфенов Николай Петрович, Алексеев Сергей Алексеевич, Стахно Роман Евгеньевич, Яковлева Наталья Александровна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: parfenov-nikolai@mail.ru

Аннотация. В структуру методики проведения практических занятий специалистов по безопасности информационных технологий в правоохранительной сфере введены термины обобщенной и частной профессиональных задач, определены совокупность показателей для оценки качества практических занятий, а также алгоритм адекватных методов обучения с использованием компьютерных средств.

Ключевые слова: проведение; содержание; процесс; технологии; качество; обучение; модели управления; учебно-материальная база; практические занятия.

INNOVATIVE METHODS OF TRAINING OF SPECIALISTS ON SAFETY OF INFORMATION TECHNOLOGIES IN THE LAW-ENFORCEMENT SPHERE

Parfyonov Nikolay, Alekseev Sergey, Stakhno Roman, Yakovleva Natalya
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mail: parfenov-nikolai@mail.ru

Abstract. Terms of the generalized and private professional tasks are entered into structure of a technique of carrying out a practical training of security specialists of information technologies in the law-enforcement sphere, defined set of indicators for an assessment of quality of a practical training, and also algorithm of adequate methods of training with use of computer means.

Keywords: carrying out; contents; process; technologies; quality; training; models of management; educational material resources; practical training.

Введение.

В структуру методики проведения практических занятий специалистов по безопасности информационных технологий в правоохранительной сфере введены термины обобщенной и частной профессиональных задач, определены совокупность показателей для оценки качества практических занятий, а также алгоритм адекватных методов обучения с использованием компьютерных средств.

Улучшение качества практических занятий (КПЗ) будущих специалистов по безопасности информационных технологий в правоохранительной сфере в высших учебных заведениях МВД связано с тем, что действенное управление КПЗ невозможно без перехода от субъективных описаний объектов, явлений, происходящих на практических занятиях (ПЗ), к строгим и объективным их представлениям. Вышеупомянутый переход возможен лишь при использовании адекватных моделей. Востребованные потребности практической подготовки специалистов делают эту задачу актуальной с позиций моделирования управления КПЗ, т.е. с установлением содержания, структуры и функций управления, а также обоснованием расчетным путем критериев эффективности ПЗ в целом и отдельных его составляющих.

Общеизвестно, что задачи системы управления качеством практических занятий (СУ КПЗ), требуют применения аналитических методов описания элементов и их взаимодействия в системе ПЗ. Лучше всего подходят методы математического моделирования, сочетающие качественные нюансы объекта моделирования с его количественными характеристиками. Модели математические позволяют аналитически оценить различные варианты управления КПЗ, осуществляемых СУ КПЗ.

Для моделирования структуры и процесса работы СУ КПЗ были проанализированы составляющие структурного, функционального и структурно-функционального подходов [1].

Проведенный анализ выявил преимущественные составляющие структурно-функционального подхода как к построению моделей системы ПЗ, так и моделей СУ КПЗ [2].

В системе ПЗ необходимо и достаточно рассмотреть следующие моделируемые объекты:

- специалист - как субъект и объект ПЗ;
- содержание ПЗ, которое документально организовано и зафиксировано;
- технология ПЗ;
- технология оценки качества и контроля на ПЗ);
- преподаватель, проводящий занятие, - как организующее и управляющее начало ПЗ, работающее в контуре автоматизированной СУ КПЗ.

Любой из вышеназванных объектов многомерен и служит определенным предметом исследования отдельных дисциплин (педагогики, социологии, физиологии, психологии, экономики и др.). Важным для моделирования на основе структурно-функционального подхода является специфическое содержание, проявляющееся у рассматриваемых объектов в динамике. Взаимодействуя, вышеназванные объекты образуют

новый сложный объект – ПЗ, управляемый СУ КПЗ. В связи с этим не приемлема любая концепция моделирования ПЗ под управлением СУ КПЗ, которая исключает любой объект из рассмотрения. В определенной форме любой из вышеназванных объектов должен занять свою нишу в теоретической схеме разработки метода управления КПЗ в высшем учебном заведении МВД.

Для отбора адекватных моделей элементов СУ КПЗ используются определенные критерии для оценки значимых свойств синтезированной СУ КПЗ в рамках контроля над эффективностью ПЗ.

По общепринятой методике, задача разработки критериев оценки эффективности функционирования элементов системы ПЗ не может быть решена, пока СУ КПЗ не прошла стадию постановки.

Для создания оптимальной СУ КПЗ, наиважное значение имеют профессиональные и личностные свойства выпускника высшего учебного заведения МВД – специалиста по безопасности информационных технологий в правоохранительной сфере. В связи с этим необходимо разработать научно-обоснованную модель специалиста [2,5,6,7,8]. На данный момент существует около 50 методик моделирования деятельности специалиста. Данный факт свидетельствует о недостаточном исследовании задач моделирования в управлении качеством подготовки и профессиональным использованием специалистов по безопасности информационных технологий в правоохранительной сфере.

В настоящее время распространены методики построения обобщенной модели специалиста, предназначенные для решения частных задач в рамках направления подготовки или специальности. Важной задачей в данных методиках является установление показателей подготовки, обеспечивающих необходимый уровень профессионального соответствия специалиста установленным требованиям к качеству его подготовки. Практически очень сложно перевести данные из области профессиональной деятельности специалистов МВД в сектор их подготовки, на язык программ, методик и учебных планов.

Повышение КПЗ зачастую определяется оптимальной разработкой содержания ПЗ и учебных программ подготовки будущих специалистов МВД. Недостаточная эффективность решения будущими специалистами задач ПЗ является следствием необоснованного отбора содержания ПЗ. Научно-обоснованная разработка метода отбора и структуризация содержания ПЗ устраняет эту причину.

Проведенный аналитический разбор существующей литературы [3,4] позволил установить, что наиглавным является переход от системы целей деятельности будущего специалиста по безопасности информационных технологий в правоохранительной сфере к системе целей ПЗ.

Для осуществления данного перехода необходимо ввести два понятия:

– обобщенная профессиональная задача – это общая (для многих ситуаций) задача МВД, которую должен научиться решать будущий специалист в ходе ПЗ;

– частная профессиональная задача – это учебная задача МВД в конкретной ситуации.

Поэтому система обобщенных профессиональных задач МВД должна быть включена в модель деятельности специалиста по безопасности информационных технологий в правоохранительной сфере, а система частных профессиональных задач - в модель содержания ПЗ. Выполненный анализ требований к отбираемому учебному материалу для проведения ПЗ позволил оценить качество содержания ПЗ определенным набором показателей

$$K_C^{\text{ТП}} = \langle M, I, P, C, D \rangle, \quad (1)$$

где: M – показатель полноты содержания ПЗ,

I – показатель информационного объема содержания ПЗ,

P – показатель посильности для обучающихся содержания ПЗ,

C – показатель сложности содержания ПЗ,

D – показатель трудности содержания ПЗ.

Полнота содержания ПЗ основывается на понятии ориентировочная основа действия (ООД) - правила и методы реализации деятельности специалиста по безопасности информационных технологий в правоохранительной сфере при выполнении любого действия, образующего алгоритм операторской деятельности МВД.

В зависимости от способа использования учебной информации (репродуктивный – все ООД известны, продуктивный – создание новых ООД и уровня усвоения деятельности (α)) содержание ПЗ различается, что иллюстрирует таблица 1.

Таблица 1

Содержание ПЗ в зависимости от способа использования учебной информации и уровня усвоения деятельности

Характеристика ООД	Способы использования учебной информации и уровни усвоения деятельности			
	Репродуктивный способ		Продуктивный способ	
	Операционный	Функциональный	Конструктивный	Творческий
Глубина ООД для решения учебной задачи	Только внешние признаки ООД, необходимые для решения учебной задачи	Обобщенные признаки ООД для жестко заданных условий решения учебной задачи	Принципы, методы и алгоритмы построения новой ООД для решения учебной задачи	Исследовательские методы, модели, алгоритмы создания принципиально новой ООД для решения учебной задачи

Полнота представления ООД (учебной задачи) в содержании ППЗ	Цели, полное описание ситуации и структура частных решений	Цели, полное описание ситуации, структура типовых решений, примеры частных решений	Цели, неполное описание ситуации, структура общих решений, примеры типовых решений	Цели в общем виде, неполное описание ситуации, методы, модели, алгоритмы поиска решений

Соотношения и характеристика входящих в них переменных для определения значений приведенных выше семи показателей оценки качества содержания ПЗ представлены в табл. 2.

Таблица 2

Соотношения и переменные для оценки качества содержания ПЗ

Показатель качества содержания ПЗ	Соотношение	Характеристика переменных
Полнота	$M = N/L$ $0 \le M \le 1$	N – множество учебных (частных) задач, L – множество обобщенных задач реальной деятельности
Информационный объем	$I = Q_Д / Q_Ф$ $0 \le I \le 1$	$Q_Д$ - дидактический объем учебного материала, $Q_Ф$ - фактический объем учебного материала
Посильность для овладения материала будущим специалистом	$P = T_{TP} / T_Ф$ $0 \le P \le 1$	T_{TP} - время, требуемое на ПЗ, $T_Ф$ - время, фактически отведенное на ПЗ
Сложность	$C = A_{С.ТП} / A_{ОБ}$ $0 \le C \le 1$	$A_{С.ТП}$ - ступень абстракции содержания ПЗ, $A_{ОБ}$ - ступень абстракции в опыте обучающегося
Трудность	$D = \alpha_{ОБ} / \alpha_{С.ТП}$ $0 \le D \le 1$	$\alpha_{ОБ}$ - опыт обучающегося, измеренный по уровню усвоения деятельности, $\alpha_{С.ТП}$ - целевой уровень усвоения деятельности по содержанию ПЗ

Примечание к таблице 2:

дидактический объем учебного материала может быть определен по формуле, введенной В.П. Беспалько

$$Q_Д = \frac{N\Delta(\alpha - \beta)H_\gamma}{1 - K_\tau} \quad (2);$$

при определении посильности овладения обучающимся содержания ПЗ может быть использованы следующие соотношения:

$T_{TP} > T_Ф$ – не посильно, перегрузка будущего специалиста,

$T_{TP} = T_Ф$ – посильно при полной нагрузке,

$T_{TP} < T_Ф$ – посильно, недогрузка будущего специалиста;

степень абстракции – научное описание деятельности, которое требует, в соответствии с дидактическими принципами научности обучения, представления учебного материала на возможно более высокой ступени абстракции, но доступной для обучающегося определенного уровня интеллектуального развития.

Осуществленный анализ разработанных моделей, которые могут служить основой для разработки структурно-функциональных частных моделей объектов системы ПЗ при подготовке специалистов по безопасности информационных технологий в правоохранительной сфере показал, что необходимо создание новых подходов к разработке адекватных моделей управления качеством содержания ПЗ, предлагающих регулирование ПЗ с помощью системы управления качеством содержания ПЗ на основе критериев и показателей качества элементов организационной и дидактической подсистем, учета характера их взаимодействия и факторов, оказывающих наибольшее влияние на управление качеством ПЗ.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев С.А., Парфенов Н.П., Пономаренко А.В. Модель управления качеством содержания практических занятий// Материалы Круглого стола от 30.04.2014г. в СПбУ МВД России.
2. Беспалько В.П. Слагаемые педагогической технологии / В.П. Беспалько. - М.: Педагогика, 1989. - 190с.
3. Ефремов О.Ю. Педагогика: Учебное пособие / О.Ю. Ефремов. - СПб.,: Питер, 2010. – 352 с.
4. Краевский В.В. Методология педагогики: новый этап: учебное пособие для студентов высших учебных заведений/ В.В. Краевский, Е.В. Бережнова. – М., Издательский центр «Академия», 2006. – 400с.
5. Модель специалиста XXI века в контексте модернизации высшего образования // Материалы Всерос. науч.- метод. конф., 15-17 сент. 2004 г., г. Туапсе. - Тюмень: Изд-во ТюмГУ, 2004. – 113 с.
6. ГОСТ Р 50922-2006. ... Федеральный закон от 27.07.2006 г. № 149-ФЗ. Об информации, информационных технологиях и о защите информации.
7. Петрунева Р.М. Модель специалиста-инженера: от деятельности к компетентности: Монография / Р.М. Петрунева; - Волгоград: Политехник, 2007. - 143 с.: ил.
8. Домбровская Л.А., Пономаренко А.В. Рабочая учебная программа «Информатика и информационные технологии в правоохранительной деятельности 10.05.05 (090915.65) Безопасность информационных технологий в правоохранительной сфере./СПб, СПбУ МВД России, 2013г.

УДК 378.1

ИНФОРМАТИКА КАК ОСНОВА ФУНДАМЕНТАЛЬНОЙ ПОДГОТОВКИ РАЗРАБОТЧИКОВ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ

Советов Борис Яковлевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: bysovetov@mail.ru

Аннотация. Отечественное образование всегда отличалось от зарубежного фундаментальностью. В течение последних пятнадцати лет высшее образование было сориентировано на западные стандарты «Болонского процесса» и вместо инженеров выпускали бакалавров и магистров, что обосновывалось необходимостью вхождения в мировую образовательную систему. Выпускники высшей школы оказались неспособными адаптироваться к нуждам отечественной промышленности, и встала проблема смены вектора развития высшего образования в сторону специалитета. Текущий век войдет в историю человечества как век информатизации, век завершения построения информационного общества во всем мире. Мы вошли в эпоху цифровой экономики. На рынке труда возникли десятки тысяч вакансий инженеров нового типа - цифровых инженеров. 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, оказалась до настоящего времени не решенной. Возникла острая необходимость подготовки специалистов для отечественной промышленности, способных адаптироваться в условиях рынка к быстро меняющимся требованиям работодателей. Эту задачу можно решить путем перехода от уровневой подготовки к специалистету при условии значительной фундаментализации образования. В условиях цифровой экономики в основу подготовки разработчиков информационных систем и технологий должен быть положен фундаментальный курс «Информатика». Этот курс должен поддержать профессию и дать выпускнику фундаментальные основы, позволяющие ему учиться в течение всей жизни.

Ключевые слова: фундаментальное образование; информатика; цифровая экономика; ключевые компетенции.

INFORMATICS AS BASIS OF FUNDAMENTAL TRAINING OF DEVELOPERS OF INFORMATION TECHNOLOGIES AND SYSTEMS

Sovetov Boris
Saint Petersburg Electrotechnical University «LETI»
5 Professor Popov Str., St. Petersburg, 197376, Russia
e-mail: bysovetov@mail.ru

Abstract. Domestic education always differed from foreign in fundamental nature. Within the last fifteen years the higher education has been oriented on the western standards of «Bologna Process» and instead of engineers let out bachelors and masters that located by need of entry into world educational system. Graduates of the higher school have appeared incapable to adapt to needs of the domestic industry, and there was a problem of change of a vector of development of the higher education towards a specialist programme. 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. We have entered an era of digital economy. In labor market there were tens of thousands of vacancies of engineers of new type - digital engineers. 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 was not solved so far. There was an urgent need of training of specialists for the domestic industry, capable to adapt in the conditions of the market to quickly changing requirements of employers. This problem can be solved by transition from-level preparation for a specialist programme on condition of considerable fundamentalization of education. In the conditions of digital economy the fundamental course «Informatics» has to be put in a basis under cooking of developers of information systems and technologies. This course has to support a profession and give to the graduate the fundamental bases allowing I eat at to study during all life.

Keywords: fundamental education; informatics; digital economy; key competences.

Характерным отличием отечественного образования всегда была его фундаментальность. Это позволяло выпускнику достаточно легко адаптироваться к различным рабочим местам и требованиям работодателя. С 2003 г. был постепенно реализован переход высшего образования на «болонскую систему» и вместо специалистов Российская высшая школа в основном была сориентирована на подготовку бакалавров и магистров. Целесообразность такого перехода обосновывалась необходимостью вхождения Российской системы образования в мировую образовательную систему. В итоге подготовка кадров в высшей школе приобрела узко профессиональный характер, и возникли значительные трудности с трудоустройством выпускников на конкретные рабочие места по причине несоответствия направленности подготовки и требований конкретного работодателя. Проведенная актуализация содержания федеральных государственных образовательных стандартов высшего образования (ФГОС 3++) с целью сопряжения с утвержденными профессиональным стандартам явилась несомненно временной мерой. По своей идее вряд ли можно считать оправданным

приспосабливать федеральные государственные стандарты высшего образования под профессиональные стандарты среднего профессионального образования, учитывая кратковременность существования последних и объективно непрерывное возникновение новых. Необходимо коренное изменение подхода к целям и содержанию высшего образования. К этому нас принуждают и внешние, и внутренние причины. К внешним – относятся санкции западных стран, что привело к необходимости импортозамещения, к внутренним - завершение построения информационного общества и вхождение страны в эпоху цифровой экономики. Принятая Правительством РФ программа по цифровой экономике предусматривает подготовку компетентных специалистов, что вызывает необходимость изменения вектора развития Российского высшего образования в направлении перехода к специалитету. В стране возникли десятки тысяч вакантных рабочих мест специалистов, в том числе цифровых инженеров. Таким образом, высшая школа должна готовить кадры для нужд российской промышленности. Перестройку содержания высшего образования целесообразно осуществить на базе лучших традиций отечественного образования. Высокое качество отечественного образования определялось его фундаментальностью.

Подготовка разработчиков информационных систем и технологий осуществляется в настоящее время в рамках направления «Информационные системы и технологии». Основой фундаментальной подготовки будущих цифровых инженеров этого направления составляет «Информатика».

В основе начального этапа возникновения информатики лежала теория информации, базирующаяся на исторической работе К. Шеннона «Статистическая теория связи», в которой были введены определения скорости передачи информации и пропускной способности канала связи. Скорость передачи информации была впервые определена вне связи со временем и отражала физически плотность информации как количество информации в символе кода. Неформально доказанная прямая теорема Шеннона позволила заложить фундаментальное условие передачи информации по каналу с шумом с бесконечно малой вероятностью ошибки. Обратная теорема Шеннона задает нижнюю границу вероятности ошибки при передаче сообщений в случае, когда производительность источника превышает пропускную способность канала связи. Интенсивное развитие теории связи и вычислительной техники привело к необходимости разработки фундаментальных основ информатики.

В структуре информатики в настоящее время обобщенно можно выделить три уровня: нижний – физический, включающий программно-аппаратные средства вычислительной техники и техники связи, средний – логический, включающий информационные и коммуникационные технологии и верхний – прикладной, включающий информационные системы различного назначения. Н. Винер предвидел интенсивное развитие информационных технологий и предсказал, что 21 век станет веком информатики, веком вхождения человечества в информационное общество. Предсказание Винера сбылось, завершается формирование информационного общества, включающего информационную экономику и информационную среду обитания человека.

Бурное развитие получили информационные технологии, и их доля в ВВП России должна значительно возрасти, что предусмотрено программой по цифровой экономике. Чтобы решить эту задачу, необходимо существенно изменить содержание подготовки разработчиков информационных систем и технологий и, в том числе, усилить его фундаментальность. В основу дисциплины «Информатика» должна быть положена классическая теория информации, включающая в себя ряд фундаментальных разделов: фундаментальные теоремы Шеннона, информационные пределы избыточности для дискретных каналов связи с независимыми и пакетными ошибками, математические основы и примеры кодирования в каналах связи без шума и с шумом. При этом особое внимание следует уделить построению систематических, циклических кодов, непрерывных кодов, псевдослучайных последовательностей и их практической реализации в рамках современных информационных технологий. Логический уровень информатики составляют современные информационные технологии. Ввиду их многообразия целесообразно подойти к их изложению с позиции теории информационных процессов, выделив типовые информационные процессы и пути построения на их основе конкретных информационных технологий. Важно довести до студентов и основы оценки качества функционирования типовых информационных процессов. Возникшая из теории связи фундаментальная теория информации основное внимание уделяет проблеме передачи информации в условиях действия внешних случайных и специально организованных помех. Отсюда необходимо в содержание дисциплины «Информатика» ввести разделы по проблемам избыточности передаваемой информации, проблемам оценки и обеспечения помехоустойчивости передачи. Фундаментальность должна поддерживаться корректными математическими доказательствами и выводами. Дисциплина «Информатика» должна заложить фундаментальные основы подготовки инженера для цифровой экономики. Пятый раздел программы «Цифровая экономика» предусматривает подготовку компетентных специалистов, способных удовлетворять требованиям, предъявляемым к цифровому инженеру.

В условиях компетентностного подхода дисциплина «Информатика» должна сформировать значительную долю профессиональной компетенции выпускника. В настоящее время предстоит ответственная работа по формулировке ключевых компетенций цифрового инженера. Решение этой задачи возможно при принятии принципиального государственного решения по изменению вектора развития Российского высшего образования с его ориентацией не на западные стандарты, а на нужды отечественной промышленности. Профессиональная компетенция, заложенная в данной дисциплине, должна органично сочетаться с другими профессиональными и общекультурными компетенциями специалиста в области цифровой экономики. Фундаментализация высшего образования должна способствовать более быстрой адаптации выпускника ВУЗа к меняющимся требованиям работодателя в условиях развивающейся цифровой экономики.

Выделяют разное количество компетенций, которые должны быть сформированы в процессе обучения, но независимо от их числа они должны содержательно включать: готовность к проявлению компетентности (мотивационный аспект), владение знанием содержания компетентности (когнитивный аспект), опыт проявления компетентности в разнообразных стандартных и нестандартных ситуациях (поведенческий аспект), отношение к содержанию компетентности и объекту ее приложения (ценностно-смысловой аспект). В компетентностной модели цели образования связываются как с выполнением конкретных функций, так и с междисциплинарными интегрированными требованиями к результату образовательного процесса.

Цель профессионального образования состоит в широком смысле в том, чтобы приобрести компетентность, которая позволяет выпускнику адаптироваться к рынку труда. Обращение к оценке качества образования через компетенцию означает, что образование тесно связывается с «трудоустройством». Компетенции предполагают возможность использования знаний выпускника в ряде профессий. Для отечественной системы образования переход к системной модели (квалификационной и компетентностной в их единстве) представляется крайне актуальным.

Российская система образования всегда была компетентностной, т.е. ориентированной на сферу профессиональной деятельности, но она была ориентирована на подготовку специалистов для массового и стабильного производства. В настоящий период от системы высшего образования ожидается подготовка выпускников, которые могут заниматься как поиском работы, так и выступать в роли создателей рабочих мест. Модель должна носить системный характер, объединяя преимущества квалификационной и компетентностной моделей. Реализация системной модели требует получения результатов обучения в двух направлениях: квалификационно-профессиональном и в междисциплинарно-компетентностном. 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 приводит к необходимости формирования ноосферной модели образования. Общими лозунгами и научными рассуждениями здесь вряд ли удастся ограничиться. Нужно изменение подхода на политическом уровне к образованию.

Советское образование по праву можно считать ноосферным, оно включало в себя воспитание и обучение. Отработанная система воспитания подрастающего поколения в образовательных учреждениях, включающая в себя серьезную вне учебную работу, была ориентирована на нравственные ценности. В рамках высшего профессионального образования была сложившаяся практика: ВУЗ-НИИ-производство. Молодежь стремилась к интересной духовно наполненной работе. Многие элементы советского образования как фундаментального необходимо возродить на новом уровне с учетом внешних и внутренних возмущающих воздействий. Наряду с новыми ключевыми компетенциями цифровой экономики необходимо ввести ноосферную составляющую в общекультурные компетенции. Это позволит обеспечить приоритетность воспитания в учебно-образовательном процессе и сформировать у выпускников ВУЗов способность к непрерывному обучению в течение всей жизни как в условиях рынка, так и в условиях плановой экономики.

СПИСОК ЛИТЕРАТУРЫ

1. Б.Я. Советов О развитии инженерного образования и подготовок IT специалистов для цифровой экономики. // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 5 / СПОИСУ. – СПб., 2018. – 549 с. С. 310-314.
2. 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. – 148 с.

УДК 378.016:004

ПРОБЛЕМЫ МЕТОДИКИ ПРЕПОДАВАНИЯ ИНФОРМАТИКИ В ШКОЛАХ ЛИНГВИСТИЧЕСКОГО ПРОФИЛЯ

Фёдоров Константин Павлович[1]
Санкт-Петербургский государственный университет,
Колледж физкультуры и спорта, экономики и технологии
Измайловский пр., 27, Санкт-Петербург, 190005, Россия
e-mail: constantin325@rambler.ru

Аннотация. Рассмотрены основные проблемы методики преподавания информатики, с которыми сталкиваются учителя, работающие в школах лингвистического профиля. Проанализированы возможные пути решения данных проблем.

Ключевые слова: межпредметные связи информатики и иностранных языков; вариативность содержания обучения; дифференциация задач по уровням сложности обучения; учет особенностей конкретного иностранного языка; оценивание эффективности методики преподавания.

THE PROBLEMS OF THE METHODICS OF TEACHING INFORMATICS AT SCHOOLS OF LINGUISTIC PROFILE

Fyodorov Konstantin
St. Petersburg State University,
College of Physic Culture and Sport, Economic and Technology
27 Izmaylovsky Av., St. Petersburg, 190005, Russia
e-mail: constantin325@rambler.ru

Abstract. The main problems of the methodics of teaching informatics faced by teachers working in schools of linguistic profile. Possible ways of solving these problems are analyzed.

Keywords: interdisciplinary communications of the informatics and foreign languages; the variability of the studying content; differentiation of tasks for levels of complexity of studying; accounting peculiarities of a certain foreign language; the evaluation of the efficiency of teaching methodics.

Проблемы методики преподавания информатики рассматривались в исследованиях ряда авторов, среди которых следует выделить И. Г. Семакина, Н. Ю. Пахомову, Р. Р. Камалова, Л. В. Галыгину, Л. Л. Босову, Т. В. Николаеву, А. В. Горячева, А. Л. Богачева, А. В. Рябых, В. П. Линькову, Р. И. Баженова, С. М. Окулова, А. В. Якушина, В. П. Шумилина, А. В. Ковригина, М. Л. Белобородову, М. А. Манасытову, О. М. Толстых. Анализ трудов перечисленных исследователей позволяет сделать вывод, что преподавание информатики в российских школах, вне зависимости от их профиля, осуществлялось ранее и осуществляется в настоящее время согласно стандартной методике преподавания данной дисциплины, основанной на системе традиционного обучения и не учитывающей особенностей профиля конкретного учебного заведения.

Система традиционного обучения прежде всего подразумевает классно-урочную организацию обучения, сложившуюся в XVII в. на принципах дидактики, сформулированных чешским педагогом Я. А. Коменским [9] и до сих пор преобладающую в большинстве школ мира. М. А. Мкртчян [14] выделяет главные характеристики системы традиционного обучения:

Учащиеся делятся на классы – учебные группы, постоянные (или почти постоянные) по составу. Дифференциация по уровню обучения отсутствует. В каждый конкретный момент времени все ученики одного класса изучают одну и ту же определенную тему курса некоторой дисциплины согласно одним и тем же методикам преподавания и обучения.

Основу системы традиционного обучения составляет традиционная технология обучения, обеспечивающая процесс передачи знаний, умений и навыков (ЗУН), а также опыта от учителя к ученикам. Этот процесс включает в себя цели, содержание, методы и средства обучения.

Главной целью традиционной технологии обучения является формирование системы знаний и овладение основами наук. Официально декларируется всестороннее развитие личности, однако фактически данному аспекту не уделяется должного внимания.

Содержание обучения практически единообразно и неинвариантно. Базовые учебные планы основаны на стандартах, единых для всей России – федеральных государственных образовательных стандартах (ФГОС). Особенности профиля учебного заведения не учитываются или учитываются в недостаточной степени. Межпредметные связи (в частности, связи профильных дисциплин с дисциплинами других научных циклов) не реализуются совсем или реализуются лишь в минимальном объеме.

Учитель использует в своей профессиональной деятельности традиционные методы обучения, целью которых является сообщение учащимся новых знаний и доведение до них актуальной информации по изучаемой дисциплине. Такие методы основаны на деятельности информативно-иллюстративного (объяснительно-иллюстративного, информационно-рецептивного) характера со стороны педагога и репродуктивной деятельности учащихся.

Главной особенностью традиционных методов обучения является то, что они основаны на сообщении учащимся готовых знаний, обучении по стандартному образцу, индуктивной логике от частного к общему, механической памяти, вербальном изложении учителя и репродуктивном воспроизведении учащимися.

Особенностью традиционной методики обучения, применяемой в системе традиционного обучения и основанной на традиционных методах обучения, является авторитарная педагогика требований. Авторитаризм процесса обучения проявляется в регламентации деятельности учащихся, принудительности обучающих процедур, централизации контроля и ориентации на среднестатистического ученика. Практически отсутствуют условия для раскрытия индивидуальных способностей учащихся, творческих проявлений личности.

Процесс обучения как деятельность в традиционной системе обучения характеризуется отсутствием самостоятельного целеполагания учащихся, поскольку цели обучения ставит учитель. Планирование учебной деятельности ведется извне, навязывается ученику вопреки его желанию. Итоговый анализ и оценивание деятельности ребенка производятся не им, а учителем. В этих условиях этап реализации учебных целей обычно превращается в труд “из-под палки” со всеми его негативными последствиями, вплоть до полного отчуждения некоторых учеников от учебы.

Анализ особенностей системы традиционного обучения позволяет выявить положительные и отрицательные стороны системы традиционного обучения. Они представлены в таблице 1.

Таблица 1

Положительные и отрицательные стороны системы традиционного обучения

Положительные стороны	Отрицательные стороны
Систематический характер обучения. Упорядоченная, логически обоснованная подача учебного материала. Организационная четкость учебной деятельности учителя и учащихся. Постоянное эмоциональное воздействие личности учителя на учащихся. Минимальные затраты педагогических ресурсов (но не учебного времени) при массовом обучении.	Шаблонное построение и однообразие подачи учебного материала. Нерациональное распределение учебного времени. Обеспечение лишь первоначальной ориентировки учащихся в материале, изучаемом на уроке, и перекладывание более высоких уровней его усвоения на домашние задания (которые далеко не все выполняют). Пассивность или лишь видимость активности учащихся на уроке. Изоляция учащихся от тематического общения друг с другом и слабость речевой активности учащихся на занятиях. Ориентация на “среднестатистического ученика”, отсутствие самостоятельности и возможностей самореализации личности учащихся. Низкий уровень обратной связи учащихся с учителем. Отсутствие возможностей индивидуального обучения. Отсутствие вариативности содержания обучения и, следовательно, ограниченность возможностей адаптации содержания к профилю образовательного учреждения. Ограниченность возможностей реализации межпредметных связей различных учебных дисциплин.

Недостатки системы традиционного обучения и их преобладание над ее достоинствами способствуют возникновению ряда проблем в профессиональной деятельности педагогов, использующих данную систему обучения. В профильных учебных заведениях, к категории которых относятся школы с углубленным изучением иностранных языков, учителя информатики должны решить следующие проблемы методики преподавания данной дисциплины:

Концепция профильного обучения [10] предписывает учитывать профиль учебного заведения (в данном случае – лингвистический) и строить методики преподавания учебных дисциплин других циклов (в частности, методику преподавания информатики) с учетом обеспечения возможностей реализации межпредметных связей исследуемой и профильной дисциплин (т. е. информатики и иностранных языков). Однако содержание в системе традиционного обучения (см. п. 4 особенностей данной системы) не учитывает особенности профиля школ с углубленным изучением иностранных языков и не обеспечивает возможности реализации межпредметных связей информатики и иностранных языков. Ни одна из стандартных программ по информатике для средней школы [16] не обеспечивает в явном виде возможностей реализации межпредметных связей информатики и иностранных языков (т. е. межпредметных связей исследуемой и профильной дисциплин), рекомендуемых образовательными стандартами [15, 17] и Концепцией профильного обучения [10, 12]. В программы по информатике и ИКТ не включено изучение программных средств и информационных технологий, предназначенных для организации телеконференций с носителями языка, сетевых форумов и семинаров, посвященных иностранным языкам либо вопросам лингвистики, просмотра иностранных фильмов на языке оригинала, диалогов и группового общения на иностранных языках. На изучение систем машинного перевода текстов и электронных словарей отводится лишь несколько часов в течение всего курса обучения информатике в школе. Кроме того, при обучении информатике по стандартным программам не проводятся параллели между иностранными языками и языками программирования, не изучается терминология в области информатики на иностранных языках, не реализуются другие возможности применения учащимися знаний, умений и навыков (ЗУН) из области иностранных языков для решения задач курса информатики, т. е. не реализуются обратные межпредметные связи информатики и иностранных языков. Данный факт можно объяснить тем, что стандартные программы по информатике являются программами общего образования и не адаптированы к какому-либо конкретному профилю (исключение составляют программы курса информатики профильного уровня на ступени среднего (полного) общего образования, но они ориентированы не на лингвистический, а на информационно-технологический профиль) [23, 29].

Российский Федеральный государственный образовательный стандарт (ФГОС) [15] официально декларирует всестороннее развитие личности и рекомендует дифференциацию уровней обучения учащихся в

соответствии с их возможностями и способностями. Концепция профильного обучения [10] содержит требование адаптации программ по дисциплинам, не входящим в профильный цикл, к профилю учебного заведения. Однако стандартная методика преподавания информатики, основанная на системе традиционного обучения, подразумевает жесткую привязку содержания обучения к официальным учебным планам в строгом соответствии с ФГОС, отсутствие вариативности содержания обучения и дифференциации сложности заданий по уровням обучения, шаблонное построение учебного материала, отсутствие самостоятельности учащихся и ограниченность возможностей самореализации личности учащихся, изоляцию учащихся от тематического общения друг с другом и слабость речевой активности учащихся на занятиях (что особенно неприятно в языковых школах). Перечисленные недостатки системы традиционного обучения приводят к тому, что возможности адаптации содержания обучения информатике к профилю школ с углубленным изучением иностранных языков и реализации межпредметных связей информатики и иностранных языков при обучении информатике по системе традиционного обучения сильно ограничены.

Жесткая стандартизация программ по информатике означает, в частности, что профессиональная терминология в области информатики изучается в стандартном формате, т. е. с использованием терминов англоязычного происхождения. В школах с углубленным изучением других языков (немецкого, французского, финского и др.) не учитываются особенности конкретного языка и не изучается терминология в области информатики на языке, изучаемом в данной школе.

Требования к результатам освоения программы по информатике учащимися, предъявляемые ФГОС и, в профильных учебных заведениях – Концепцией профильного обучения, подразумевают, что учитель должен периодически контролировать уровень выполнения этих требований и, в конечном итоге, контролировать эффективность применяемой методики преподавания информатики. Анализ работ ряда исследователей (С. И. Архангельский, Г. И. Батурина, Т. Ф. Кузина, В. П. Беспалько, В. М. Блинов, И. Я. Лернер, В. П. Мизинцев, М. Н. Скаткин) позволил сделать вывод, что системы оценивания эффективности методик преподавания и обучения, предложенные перечисленными авторами, используют недостаточно строгие алгоритмы расчета числовых значений критериев эффективности и, кроме того, не учитывают факторы динамики показателей качества учебного процесса.

Перечисленные проблемы свидетельствуют о недостаточной эффективности стандартной методики преподавания информатики, основанной на системе традиционного обучения, предполагающей обучение данной дисциплине по стандартным программам, жестко привязанным к ФГОС и не допускающим вариативности содержания обучения, при ее использовании в школах лингвистического профиля. Автор статьи предлагает следующие пути решения данных проблем:

Расширить сферу применения прямых межпредметных связей информатики и иностранных языков можно путем более глубокого изучения на уроках информатики в школах лингвистического профиля программных средств, предназначенных для работы в области лингвистики. Кроме уже упомянутых систем машинного перевода и электронных словарей (на изучение основ работы с которыми в языковых школах следует отвести бóльшее время по сравнению с образовательными учреждениями других профилей), к таковым относятся системы, позволяющие организовать фронтальное, диалоговое и групповое общение учителя и учащихся на иностранных языках, просмотр иностранных фильмов на языке оригинала, телеконференции с носителями языка, лингвистические форумов и семинары. Для успешного овладения перечисленными программными средствами необходимо также изучать информационно-коммуникационные технологии (ИКТ), предназначенные для работы с ними.

А. С. Котов и Ж. Г. Шакуто [11] выделяют одну из возможностей реализации обратных межпредметных связей информатики и иностранных языков (т. е. возможностей применения на уроках информатики ЗУН, приобретенных в процессе освоения курса иностранного языка) - сравнительный анализ иностранных языков и языков программирования. Первые представляют собой категорию естественных языков, вторые – категорию формальных языков. Изучение технологии программирования, равно как и изучение иностранных языков, требует от учащихся наличия достаточно хорошо развитых навыков формализации. Точно так же, как предложения в естественных человеческих языках строятся по определенным правилам, степень строгости которых зависит от конкретного языка (особенно строги правила синтаксиса в немецком языке, в котором каждый член предложения занимает строго фиксированное место, и их перестановка недопустима, т. к. может привести к изменению смысла фразы [8]), таким же образом построена структура языков программирования: все конструкции должны быть описаны предельно четко и не допускают отклонений от правил. Как для правильного формирования предложений естественного языка, так и для правильного построения конструкций языка программирования необходимо четко следовать формальной логике и знать правила синтаксиса, принципы построения лексем, особенности их вхождения друг в друга. Иностранные языки, являясь естественными языками, обладают достаточной степенью формальности – синтаксические конструкции строятся по вполне определенным правилам, предусматривающим фиксированный, и притом конечный, список исключений. Следовательно, конструирование предложений в естественном языке вполне может быть формализовано и выполнено алгоритмическим путем. Составление программы также предусматривает этап формализации и выполняется алгоритмическим путем. Понимание учащимися данной аналогии позволяет более эффективно изучать основные алгоритмические структуры языков программирования и применять их на практике. С этой точки зрения языки программирования являются частным случаем иностранных языков. Поскольку иностранный язык в современной школе начинают изучать, как правило, уже с первого или со второго класса, а

алгоритмизацию и программирование – на более поздних этапах обучения, то иностранный язык может выполнять пропедевтическую функцию, являясь приготовительной базой для изучения языков программирования. Опыт, приобретенный учащимися при изучении иностранных языков, должен повысить эффективность освоения ими основ алгоритмизации и программирования. Особенно эффективным должно быть использование данной особенности обратных межпредметных связей информатики и иностранных языков в школах с углубленным изучением последних.

Кроме того, автор предлагает использовать в школах лингвистического профиля особые программы по информатике и включить в них ряд особенностей, обеспечивающих возможности реализации межпредметных связей информатики и иностранных языков:

– исследование изучаемого иностранного языка как системы (в разделе «Основы системного подхода»);

– исследование системы языков мира (в том же разделе);

– исследование системы числительных изучаемого иностранного языка (в том же разделе или в разделе «Математические основы информатики»);

– исследование иностранного языка, представляющего собой один из способов кодирования информации (в теме «Кодирование информации», входящей в состав раздела «Информация и информационные процессы»);

– анализ логических особенностей правил орфографии и пунктуации, синтаксиса и словообразования, семантических и морфологических конструкций изучаемого иностранного языка (в разделе «Основы алгебры логики»);

– построение и исследование информационных моделей семантических конструкций иностранных языков и языков программирования, политического устройства зарубежных стран, систем образования в странах изучаемых языков (в разделе «Информационное моделирование»);

– изучение научной терминологии в области информатики на изучаемом иностранном языке (если в школе на углубленном уровне изучается не английский, а другой иностранный язык, то следует уделить особое внимание изучению научной терминологии именно на этом языке. Таким образом будут учтены особенности конкретного иностранного языка, изучаемого в данной школе.), составление терминологического словаря в системе машинного перевода (в разделе “Компьютер – универсальное средство для работы с информацией”).

Владение иностранными языками не только позволяет решить задачи информатики, указанные выше и аналогичные им, но и способствует чтению в подлинниках иностранной научной литературы в области информатики и в других областях науки, возможности применения на практике знаний, почерпнутых из данной литературы, анализа и исследования изложенных в ней фактов, открытия нового, возможности изложения своих знаний представителям иноязычных народов. С другой стороны, владение информационными технологиями способствует решению ряда проблем, стоящих перед учащимися в процессе освоения иностранных языков. Поэтому задачи, позволяющие реализовать межпредметные связи информатики и иностранных языков, должны быть включены в содержание курса программ по информатике, предназначенных для школ лингвистического профиля.

Поиск путей преодоления трудностей, с которыми сталкиваются педагоги и учащиеся школ с углубленным изучением иностранных языков при обучении информатике по системе традиционного обучения, привел к мысли, что повысить эффективность обучения информатике в языковых школах можно путем использования в методике преподавания данной дисциплины иной системы обучения, альтернативной системе традиционного обучения и способной преодолеть недостатки последней и при этом сохранить ее достоинства.

Прежде всего учитель должен отказаться от шаблонного построения учебного материала и использовать нестандартный, творческий, креативный подход к изучению нового материала и решению практических задач, стоящих перед учащимися в процессе обучения.

Сама творческая составляющая методики преподавания уже способна привлечь учащихся к решению поставленных задач, возбудить в них интерес к изучению материала, мотивировать их к учебной деятельности. Кроме того, необходимо всячески повышать активность учащихся на уроке, больше времени уделять общению детей друг с другом и с учителем, предлагать разноуровневые задания, дифференцируя их сложность в зависимости от способностей и потребностей каждого конкретного ученика.

Одной из систем обучения, альтернативной системе традиционного обучения и обладающей свойствами, указанными в предыдущем абзаце, является *система эвристического обучения* (СЭО), включающая в себя эвристические методы, эвристические формы, эвристические технологии и эвристические программные средства обучения. СЭО берет свое начало от майевтики – методики обучения, разработанной древнегреческим философом Сократом (469 – 399 до Р. Х.).

Система Сократа основана на том, что учитель помогает ученику самостоятельно подойти к постановке и решению проблемы путем последовательного поиска ответов на специально подготовленные наводящие вопросы, порождающие цепочку ассоциативных рассуждений и организующие процесс эвристического поиска решения задачи. Из фундаментальных понятий с помощью наводящих вопросов постепенно выводятся новые понятия, определяются промежуточные результаты, и как итог отыскивается ответ на интересующий нас вопрос и достигается поставленная цель. Путь к цели долог и тернист, но цель достигнута!

Следует отметить, что благодаря эвристическому поиску истина зачастую открывается не только ученику, но и самому учителю [26, 27].

Разработчиками современной СЭО считаются А. В. Хуторской [32-33] и В. И. Андреев [3]. Исследование их трудов позволило определить основные характеристики СЭО. Основу СЭО составляют эвристические технологии обучения, главной целью которых является организация поисково-эвристической деятельности учащихся на уроке.

Данный вид деятельности развивает у обучающихся способность анализировать и систематизировать информацию на основе самоорганизации, самоуправления, самоанализа, и применять ее для решения поставленной задачи, адаптироваться к новым условиям и предвидеть ожидаемые результаты, принимать обоснованные решения на основе эвристических алгоритмов с последующей логической проверкой полученных результатов.

Поисково-эвристическая деятельность эффективна при умении обучающихся оценивать свои действия, степень их рациональности и экономичности, настойчиво доводить решение задачи до логического конца. При этом учащиеся должны обладать гибкостью мышления, способностью актуализировать, анализировать и организовать информацию в решаемой задаче. Это осуществляется на основе эвристических правил (рекомендаций к выбору возможного варианта действий в условиях альтернативного поиска) и операций (мыслительных действий, направляющие деятельность обучающегося на нахождение оптимального решения задачи), основанных на аргументированных и логически обоснованных рассуждениях [21, 32].

Особой эвристической технологией является теория решения изобретательских задач (ТРИЗ) – технология, разработанная российским ученым Г. С. Альтшуллером для решения сложных задач в технической области [1, 2].

Позднее ТРИЗ получила развитие в ряде других сфер человеческой деятельности, в т. ч. в педагогике как специальная эвристическая технология обучения, которая с успехом может быть применена для решения задач творческого характера, относящихся к компетенции различных учебных дисциплин [22, 28].

Содержание обучения по СЭО основано на ФГОС, однако в отличие от системы традиционного обучения оно допускает вариативность и предоставляет возможность адаптации программ учебных дисциплин к профилю образовательного учреждения [23, 29, 32, 33].

Учитель использует в своей профессиональной деятельности эвристические методы обучения, ставящие своей целью конструирование учащимися собственного смысла, целей и содержания образования, а также процесса его организации, диагностики и осознания. В процессе эвристического обучения ученик изначально конструирует знания в исследуемой области реальности, опираясь на личный образовательный потенциал и технологию продуктивной деятельности.

Полученный им продукт деятельности (гипотеза, сочинение, модель и т. п.) сопоставляется затем с помощью педагога с культурно-историческими аналогами, в результате чего данный продукт переосмысливается, достраивается, совершенствуется или драматизируется, вызывая необходимость новой деятельности. В данном случае неизбежно личное образовательное совершенствование учащегося через совершенствование его знаний, чувств, способностей, опыта, материальной продукции. Иногда это совершенствование является частью общекультурного совершенствования. В этом случае ученик оказывается включенным в культурно-исторические процессы в качестве их полноправного участника [3, 33].

Основными формами обучения являются эвристические формы обучения, главной целью которых является создание учащимися новых образовательных результатов.

К эвристическим формам обучения относятся эвристические уроки, олимпиады и погружения; деловые игры; предметные недели; дистанционные формы творчества (творческие работы, творческие защиты, дистанционные проекты); интерактивные формы обучения [29, 32, 33].

Для реализации эвристической методики обучения учитель должен использовать особые программные средства, которые можно назвать эвристическими программными средствами обучения. Они основаны на информационных обучающих системах, организованных в виде экспертных систем (ЭС). Алгоритмы, заложенные в основу работы ЭС, не гарантируют на сто процентов достижения поставленной цели, но, согласно многолетнему опыту использования систем данного класса, большинство учащихся успешно овладевают знаниями, умениями и навыками, преподать которые призвана система.

Таким образом, в ЭС реализованы эвристические алгоритмы, методы и технологии обучения, что обосновывает термин «Эвристические программные средства обучения» [19, 20, 24, 25, 31].

Особенностью эвристической методики обучения, применяемой в системе эвристического обучения, является ориентация на творческое начало личности, индивидуальный подход к каждому ученику, дифференциация уровней обучения в зависимости от индивидуальных способностей каждого конкретного учащегося [3, 26, 27, 30, 32].

Процесс обучения как деятельность в СЭО предоставляет возможность самостоятельного целеполагания учащихся и планирование ими учебной деятельности. Ученикам предоставляется возможность анализа, контроля и оценивания своей учебной деятельности. Уделяется внимание тематическому общению учащихся на уроке и их творческой деятельности. Совокупность перечисленных факторов является двигателем, способным мотивировать учащихся к учебной деятельности, привлечь их к решению поставленных задач, возбудить в них интерес к изучению материала [3, 26, 27, 30, 33].

Как и система традиционного обучения, СЭО имеет свои достоинства и недостатки, которые представлены в таблице 2.

Таблица 2

Положительные и отрицательные стороны системы эвристического обучения

Положительные стороны	Отрицательные стороны
1. Творческий характер обучения. 2. Рациональность использования учебного времени. 3. Разнообразие способов подачи учебного материала. 4. Высокий уровень тематического общения и речевой активности учащихся на уроке. 5. Высокий уровень обратной связи учащихся с учителем. 6. Дифференциация уровней усвоения знаний в соответствии с индивидуальными способностями и потребностями учащихся и возможность постепенного повышения упомянутых уровней. 7. Возможность проявления самостоятельности и самореализации личности учащихся. 8. Возможность индивидуального обучения учащихся (в т. ч. как особо одаренных, так и тех, кому “гранит науки” дается с трудом). 9. Вариативность содержания обучения и возможность его адаптации к профилю образовательного учреждения. 10. Возможность реализации межпредметных связей различных учебных дисциплин.	1. Отсутствие строгого логического обоснования методики обучения. 2. Недостаточный опыт апробации системы эвристического обучения. 3. Недостаточно строгая организация учебной деятельности учителя и учащихся. 4. Дополнительные затраты педагогических ресурсов и учебного времени в связи с необходимостью проверки точности результатов решения учебных задач, полученных эвристическими методами. 5. Рассеивание внимания учащихся при эвристических формах обучения. 6. Недостаточно строгий контроль знаний учащихся при организации учебных мероприятий в игровой форме.

Несмотря на ряд недостатков, главной причиной которых является недостаточная логическая строгость СЭО, данная система обладает достоинствами, позволяющими повысить эффективность обучения и способствующими самореализации личности каждого учащегося. Наиболее высокий уровень эффективности СЭО может быть достигнут в профильных учебных заведениях. Это обусловлено тем, что СЭО позволяет адаптировать содержание обучения к профилю школы и предоставляет богатые возможности реализации межпредметных связей профильных и общеобразовательных дисциплин. В частности, СЭО с успехом может быть использована при обучении информатике в школах лингвистического профиля. С помощью эвристических методов, форм и технологий обучения учащиеся под руководством учителя смогут решить сложные проблемы лингвистики средствами информационных технологий и применить лингвистические знания для решения сложных проблем курса информатики. Каким образом СЭО может быть адаптирована к лингвистическому профилю и использована в методике преподавания информатики в школах данного профиля, сказано в ряде работ автора (в частности, [19-31]).

Исследование трудов ряда исследователей, посвященных оцениванию эффективности методик преподавания и обучения [4-7, 13], позволило составить следующую таблицу, отражающую особенности систем оценивания эффективности, предложенных данными авторами (таблица 3, с. 7). По мнению автора данной статьи, система С. И. Архангельского [4] обладает наибольшей полнотой и, следовательно, именно она может быть взята за основу процесса оценивания эффективности методики преподавания информатики в школах лингвистического профиля. В данной системе учитываются многие факторы, характеризующие разнообразные аспекты эффективности методики преподавания. Но при оценивании эффективности методики преподавания информатики по системе С. И. Архангельского необходимо разрешить ряд проблем, указанных в соответствующей графе таблицы 3.

Усовершенствование системы С. И. Архангельского может быть выполнено путем объединения критериев оценки эффективности методики преподавания, используемых в данной системе, в три группы, и ее дополнения четвертой группой критериев, отражающих динамику показателей эффективности. Группы критериев эффективности в усовершенствованной системе оценивания определяются в соответствии с таблицей 4 (с. 7).

Автор предлагает выполнять оценивание эффективности методики преподавания информатики в школах лингвистического профиля по следующему алгоритму:

– Вычисление числового значения каждого критерия эффективности методики преподавания информатики в соответствии с формулами, используемыми для их расчета.

– Вычисление числового значения эффективности методики преподавания информатики по каждой группе критериев на базе оценочной функции Цермело [34], имеющей вид суммы произведений значений каждого критерия данной группы на вес критерия, отражающий степень его значимости.

– Вычисление итогового значения эффективности методики преподавания информатики на базе той же оценочной функции Цермело. На этот раз факторами, оказывающими влияние на эффективность методики преподавания в целом, считаются числовые значения эффективности по группам критериев, рассчитанные в результате выполнения второго этапа.

В работе автора [18] подробно сказано обо всех критериях эффективности методики преподавания информатики, входящих в каждую группу, и о формулах, используемых для их расчета. Достаточно простые математические действия, которые необходимо выполнить при реализации алгоритма расчета значений критериев эффективности, допускают использование ЭВМ для системного анализа эффективности методики преподавания информатики. Результат покажет уровень овладения конкретными компонентами процесса познания всеми участниками учебного процесса и в соответствии с этим позволит составить программу коррекции профессиональной деятельности преподавателя и формирования ключевых компетентностей учащихся.

Таблица 3

Системы оценивания эффективности методик преподавания и обучения

Автор системы	Критерии, используемые в системе	Проблемы, возникающие при оценивании по данной системе
В. М. Блинов	Отношение текущих результатов учебной деятельности к предельно возможным значениям соответствующих параметров.	1. Необходимость сравнения фактических результатов с неизвестным идеалом. 2. Отсутствие учета различий уровня способностей и других характеристик личности каждого конкретного ученика. 3. Отсутствие алгоритма расчета функциональной зависимости эффективности методики преподавания от значений критериев эффективности.
И. Я. Лернер	Числовые значения эффективности по четырем видам содержания обучения (знания, умения, деятельность, отношения).	1. Отсутствие механизмов поиска оптимальных пропорций, составляющих содержания обучения. 2. Необходимость точного определения веса каждой из четырех компонент.
В. П. Беспалько	1. Классификация качества усвоения знаний учащимися по шести уровням: 1) понимание; 2) узнавание; 3) воспроизведение; 4) применение; 5) творчество; 6) эвристика. 2. Коэффициент усвоения знаний. 3. Количество информации, подлежащей усвоению и обработке на данном этапе. 4. Время, затраченное на процесс достижения каждым учащимся соответствующего уровня. 5. Фактическое время выполнения данного задания каждым учащимся.	1. Критерии, используемые в системе, относятся к разным категориям (время, объем информации, усвоение знаний), и, следовательно, они не дают в явном виде числового значения эффективности методики преподавания. 2. Отсутствие строгого математического алгоритма расчета упомянутого значения. 3. Необходимость статистической обработки значений критериев, рассмотренных выше, и выражения их значений в двух формах: интервальной $x_{\min} \le x \le x_{\max}$ и среднестатистической $x_{cp} \pm \delta_x$.
С. И. Архангельский	Числовые значения критериев эффективности, разделенных на шесть групп: 1) затраты времени и труда для решения определенных задач обучения; 2) объем и качество ЗУН, приобретенных учащимися; 3) возможности методов, форм, технологий и средств обучения, используемых учителем в процессе преподавания; 4) гибкость и развитие методики преподавания в изменяющихся условиях; 5) соответствие работы педагога целям и задачам обучения; 6) качество регулирования и управления учебным процессом.	1. Отсутствие строгих методов числового расчета части критериев системы (в первую очередь это касается числовой оценки возможностей методов, форм, технологий и средств обучения, степени приспособляемости методики преподавания к изменяющимся условиям, уровня соответствия работы педагога целям и задачам обучения). 2. Отсутствие строгого алгоритма числового расчета эффективности методики преподавания по сумме всех критериев. 3. Отсутствие учета факторов динамики показателей эффективности методики преподавания (т. е. изменений их значения – улучшения, ухудшения, стабильного состояния – происходящих с течением времени). 4. Сложность расчетов в связи с разбиением критериев на слишком большое число групп.

Таблица 4

Объединение критериев системы С. И. Архангельского в четыре группы

Группы критериев эффективности по С. И. Архангельскому	Группы критериев эффективности по усовершенствованной системе	Название группы по усовершенствованной системе
1-2	1	Критерии качества обучения
3-4	2	Критерии эффективности способов деятельности участников учебного процесса
5-6	3	Критерии степени эстетического восприятия информации и ее воздействия на учащихся
–	4 (новая)	Критерии учета факторов динамики показателей эффективности методики преподавания информатики

СПИСОК ЛИТЕРАТУРЫ

1. Альтшуллер Г. С. Основы изобретательства — Воронеж: Центрально-Черноземное издательство. – 1964.
2. Альтшуллер Г. С. Творчество как точная наука.1-е изд.: М., Советское радио, 1979; 2-е изд. (дополненное): Петрозаводск, Скандинавия, 2004.
3. Андреев В. И. Эвристика для творческого саморазвития. – Казань, 1994. – 237 с.
4. Архангельский С. И. Учебный процесс в высшей школе, его закономерные основы и методы: учебно-методическое пособие – М.: Высшая школа, 1980 – 368 с.
5. Беспалько В. П. Опыт разработки и использования критериев качества усвоения знаний // Советская педагогика, 1968, №4.
6. Беспалько В. П. Слагаемые педагогической технологии – М.: Педагогика, 1989 – 190 с.
7. Блинов В. М. Эффективность обучения – М.: Педагогика, 1976 – 191 с.
8. Болдырева Л. М., Панкова О. Т., Тельнова А. Г. Самоучитель немецкого языка. М., Высшая школа, 1983.
9. Коменский Я. А. Великая дидактика. М.: Наркомпрос, 1939. – 318 с.
10. Концепция профильного обучения на старшей ступени общего образования. М., 2002.
11. Котов А. С., Шакуто Ж. Г. – Реализация межпредметных связей информатики и иностранного языка через использование компьютерных исполнителей – М., Педагогика, 2011.
12. Кривых С. В., Абдуллаева О. А., Алексашина И. Ю., Марковская Е. А. Теория и методика организации профильного обучения: Санкт-Петербургский опыт. Учебное пособие для специалистов по управлению образованием / Под редакцией И. Ю. Алексашиной – СПб, 2016 – 195 с.
13. Лернер И. Я. Дидактические основы методов обучения – М.: Педагогика, 1985.
14. Мкртчян М. А. Становление коллективного способа обучения: монография. Красноярск, 2010. С. 43-44.
15. Приказ Министерства образования и науки Российской Федерации от 17.12.2010 № 1897 “Об утверждении Федерального государственного образовательного стандарта основного общего образования” (в редакции приказа Минобрнауки России от 29.12.2014 № 1644).
16. Рабочие программы по информатике и ИКТ. 5-11 классы / авт.-сост. Т. К. Смыковская – 3-е изд., стереотип. – М.: Планета, 2010 – 224 с. – (Образовательный стандарт).
17. Рекомендации по преподаванию информатики в университетах и колледжах (Computing Curricula 2016: Computer Science) – СПб., 2016. Пер. с англ. В. Л. Павлова и А. А. Терехова.
18. Фёдоров К. П. Использование математического аппарата для усовершенствования системы (алгоритма) оценивания эффективности методики обучения информатике. Известия Российского государственного педагогического университета им. А.И. Герцена. СПб, 2016. № 179. С. 113-123. Статья ВАК. Режим доступа: https://elibrary.ru/download/elibrary_26942742_95364816.pdf.
19. Фёдоров К. П. Использование экспертных систем в качестве эвристических программных средств обучения информатике учащихся школ лингвистического профиля. В сборнике: Научно-технический прогресс: актуальные и перспективные направления будущего. Сборник материалов IV Международной научно-практической конференции. Западно-Сибирский научный центр. Кемерово, 2016. С. 83-85.
20. Фёдоров К. П. Оценка эффективности методик обучения информатике учащихся школ лингвистического профиля с помощью эвристических информационных обучающих систем. В сборнике: Искусственный интеллект: философия, методология, инновации Сборник трудов IX Всероссийской конференции студентов, аспирантов и молодых ученых. Е. А. Никитина (отв. редактор). МГТУ МИРЭА, М., 2015. С. 168-174. Режим доступа: http://www.scmaiconf.ru/public_files/2015/book-2015-sait.pdf.
21. Фёдоров К. П. Педагогические технологии организации поисково-эвристической деятельности на уроках информатики. В сборнике: Информационно-телекоммуникационные системы и технологии (ИТСиТ-2014). Материалы Всероссийской научно-практической конференции. Кемерово, 2014. С. 305.
22. Фёдоров К. П. Применение ТРИЗ на уроках информатики в школах с углубленным изучением иностранных языков / К. П. Фёдоров // Известия Российского государственного педагогического университета им. А.И. Герцена. 2017. № 185. С. 116-124. Статья ВАК. Режим доступа: http://elibrary.ru/download/50651833.pdf.
23. Фёдоров К. П. Проблема отбора содержания курса информатики для школ с углубленным изучением иностранных языков. В сборнике: Современные проблемы и тенденции развития экономики, управления и информатики в XXI веке Материалы IV ежегодной международной научно-практической конференции. СПб, 2014. С. 72-73.
24. Фёдоров К. П. Эвристические информационные обучающие системы и их использование при обучении информатике учащихся школ лингвистического профиля. В сборнике: Информационно-телекоммуникационные системы и технологии (ИТСиТ-2014). Материалы Всероссийской научно-практической конференции. Кемерово, 2014. С. 191-192.
25. Фёдоров К. П. Эвристические информационные обучающие системы и их применение на уроках информатики в школах нематематического профиля. Сборник трудов VIII Всероссийской конференции студентов, аспирантов и молодых ученых “Искусственный интеллект: философия, методология, инновации”. Е. А. Никитина (отв. редактор). МГТУ МИРЭА, М., 2014, с. 49-54. Работа награждена дипломом II степени. Режим доступа: http://www.scmaiconf.ru/public_files/2014/sbornik_2.pdf).
26. Фёдоров К. П. Эвристические методы обучения в преподавании информатики учащимся школ с углубленным изучением иностранных языков. В сборнике: VIII Международная конференция “Европейская наука и технологии”. Мюнхен, 2014.

http://spoisu.ru

27. Фёдоров К. П. Эвристические методы обучения в преподавании курса информатики и ИКТ для учащихся нематематического профиля / К. П. Фёдоров // Известия Российского государственного педагогического университета им. А.И. Герцена. 2014. № 170. С. 116-124. Статья ВАК. Режим доступа: http://elibrary.ru/download/50651833.pdf.
28. Фёдоров К. П., Абрамян Г. В. Использование элементов ТРИЗ при решении задач повышенной трудности на занятиях по информатике. В сборнике: Информационные технологии Сибири. Сборник материалов международной научно-практической конференции. Западно-Сибирский научный центр. Кемерово, 2016. С. 76-82.
29. Фёдоров К. П., Абрамян Г. В. Требования к отбору содержания программ по информатике и ИКТ для школ с углубленным изучением иностранных языков. В сборнике: Региональная информатика «РИ-2014». Материалы XIV Санкт-Петербургской международной конференции. 2014. С. 374.
30. Фёдоров К. П., Абрамян Г. В. Эвристические методы и методики обучения информатике в школах с углубленным изучением иностранных языков. В сборнике: Региональная информатика «РИ-2012». Материалы юбилейной XIII Санкт-Петербургской Международной конференции. 2012. С. 268-269.
31. Фёдоров К. П., Абрамян Г. В. Эвристические программные средства и их использование с целью развития информационно-коммуникационных компетенций учащихся школ лингвистического профиля. Российская история. 2014. Т. 2014. С. 375. Журнал входит в международную научную систему “Web of Science”.
32. Хуторской А. В. Дидактическая эвристика. Теория и технология креативного обучения. – М., издательство МГУ, 2003. – 416 с.
33. Хуторской А. В. Эвристическое обучение: теория, методология, практика. Научное издание. – М., Международная педагогическая академия, 1998. – 266 с.
34. Цермело Э. О применении теории множеств к теории шахматной игры // Матричные игры М., Физматгиз,1961, С.167–172 (оригинал: Zermelo E. Über eine Anwendung der Mengenlehre zur Theorie des Schachspiels. Proceedings of the Fifth International Congress of Mathematicians (Cambridge, 1912), Cambridge University Press, 1913, P. 501–504).

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕДИЦИНЕ И ЗДРАВООХРАНЕНИИ

УДК 616.006.6:15

ОПРЕДЕЛЕНИЕ ТИПА ЛИЧНОСТНОЙ АКЦЕНТУАЦИИ В СИСТЕМЕ ВЗАИМООТНОШЕНИЙ «ВРАЧ-ПАЦИЕНТ» В ОНКОЛОГИИ

Бланк Михаил Аркадьевич[1], Бланк Ольга Алексеевна[1], Минкин Виктор Альбертович[2], Николаенко Яна Николаевна[2]

[1] Российский научный центр радиологии и хирургических технологий имени академика А.М. Гранова Министерства здравоохранения Российской Федерации
Ленинградская ул., 70, Санкт-Петербург, 197758, Россия
[2] Многопрофильное предприятие «ЭЛСИС»
Тореза пр., 68, Санкт-Петербург, 194223, Россия
e-mails: mablank@mail.ru, oablank@mail.ru, minkin@elsys.ru, nikolyana81@mail.ru

Аннотация. Представлен первый опыт применения в клинике практически ориентированной модели экспресс-диагностики типов акцентуаций личности с целью определения психологической совместимости лечащего врача и пациента. Совместимость пациента и лечащего врача по преобладающему типу психологической акцентуации обеспечивает возможность их сотрудничества в лечении злокачественных новообразований.

Ключевые слова: психологическая акцентуация; диагностика акцентуаций; личность; лечащий врач; пациент; злокачественные новообразования

EXPRESS DIAGNOSTICS OF PERSONALITY ACCENTUATION TYPES. FIRST CLINICAL EXPERIENCE IN ONCOLOGY

Blank Mikhail[1], Blank Olga[1], Minkin Viktor[2], Nikolaenko Yana[2]

[1] Russian Research Center for Radiology and Surgical Technologies named after Academician A.M. Granov of the Ministry of Health of Russian Federation
70 Leningradskaya Str., St. Petersburg, 197758, Russia
[2] Elsys Corporation
68 Toreza Av., St. Petersburg, 194223, Russia
e-mails: mablank@mail.ru, oablank@mail.ru, minkin@elsys.ru, nikolyana81@mail.ru

Abstract. First clinical experience of using praxis aimed model of express diagnostics of personality accentuations types in the aspect of determining the psychological compatibility of the attending physician and patient is proposed. The compatibility of the patient and the attending physician according to the prevailing type of psychological accentuation provides their collaboration in the treatment of malignant neoplasms.

Keywords: accentuations of character; diagnostics of accentuations; personality; patient and doctor compatibility; malignant neoplasms.

Введение.

Современный тренд развития онкологии – персонализация подходов к лечению конкретной опухоли с учётом её молекулярных особенностей. Личность пациента в целом выпадает из поля зрения при формировании стандартов терапии. Тем не менее, психологические особенности человека, находящегося в критической ситуации смертельно опасной, с его точки зрения, болезни – фактор, во многом определяющий течение и прогноз заболевания. Доверие и активное сотрудничество лечащего врача и пациента – залог максимально достижимой эффективности лечения [1]. Важным условием продуктивного сотрудничества является психологическая совместимость людей.

Внимание к личности пациента, психотерапевтическое воздействие общения с лечащим врачом оказывают не только психологический, но и симптоматический эффект. Известно, что одним из основных тяжких симптомов злокачественной опухоли может быть боль. Боль может проявляться при любой стадии опухоли и ни в коем случае не присуща только терминальной стадии [2]. Болевой синдром существенно ухудшает качество жизни пациента. Поэтому поиск способов купирования болевого синдрома является актуальной проблемой. «Связь психической и физической боли не подлежит сомнению, если учесть, что психический компонент реализуется в таких состояниях как депрессия, тревога, страх. Сколько раз отмечалось медиками, что во время психотерапевтической беседы, нередко купирующей эти явления, больной забывал о времени очередного приёма обезболивающих» [3]. Соответственно, проблема облегчения страданий больного выходит за пределы

медикаментозного воздействия и распространяется также в область психологической совместимости личностей больного и лечащего врача.

Ранее было установлено, что тип психологической акцентуации существенным образом влияет на взаимоотношения больного и врача [3]. Определение психологического профиля человека – сложный и трудоёмкий процесс, который может вызвать негативную реакцию больного. Кроме того, загруженность врача в клинике не позволяет ему проводить длительное тестирование каждого пациента. Внедрение компьютерных методов тестирования [4], в частности для оценки тревожности [5], позволяет сделать обследование быстрым и комфортным для его участников. Более сложной задачей является создание инструментов, позволяющих производить комплексный анализ разнообразных психосоматических проявлений и особенностей психологического профиля человека, определённых путём тестирования [6, 7].

Целью настоящего этапа исследования явилось испытание методики «PsyAccent», позволяющей быстро и эффективно определять тип психологической акцентуации, в амбулаторных условиях и в условиях онкологического стационара.

Материал и методы. Материалом для исследования послужили клинические данные о 9 больных злокачественными новообразованиями и о 6 лечащих врачах. Клинико-лабораторное обследование всех больных соответствовало действующим клиническим рекомендациям. Все врачи имели высшую квалификационную категорию и были здоровы (по результатам планового ежегодного профилактического осмотра допущены к работе). Определение типа психологической акцентуации осуществлялось при помощи методики «PsyAccent», на базе технологии виброизображения [6, 8], позволяющей получать многомерные зависимости характеристик психофизиологического состояния (ПФС) и регистрировать изменение энергетики и направление этого изменения. Изменение выделяемой (расходуемой) человеком энергии при переходе из начального состояния в другое энергетическое состояние, измеряется в ккал/мин [9]. Совместимость лечащего врача и пациента определяли путём опроса пациента и с помощью методики «PsyAccent», основанной на модифицированной модели А.В.Гнездилова [3]. Шкала совместимости различных психотипов выглядит следующим образом (Табл.1).

Таблица 1

Таблица предпочтений больными врачей в различных характерологических группах (Гнездилов А.В., 1995)

Тип больного	Тип врача				
	Шизоид	Циклоид	Эпилептоид	Психастеник	Истероид
Шизоид	III	II	V	IV	I
Циклоид	V	I	II	III	IV
Эпилептоид	III	I	V	IV	II
Психастеник	III	II	I	IV	V
Истероид	I	II	III	IV	V

Модель А.В. Гнездилова была дополнена нами дистимным типом психологической акцентуации и выбрана как наиболее адаптированная к проблемам онкологических больных (Табл. 2), в отличие от моделей К.Леонгарда [10] и А.Е.Личко [11], по-разному трактующих типологию акцентуаций личности.

Таблица 2

Линейно-оппозиционная структура расположения акцентуаций личности (модель Гнездилова А.В., в модификации)

Оппозиционные типы психологической акцентуации личности	
Психастенический	Эпилептоидный
Дистимический	Истероидный
Эмотивно-циклоидный	Шизоидный

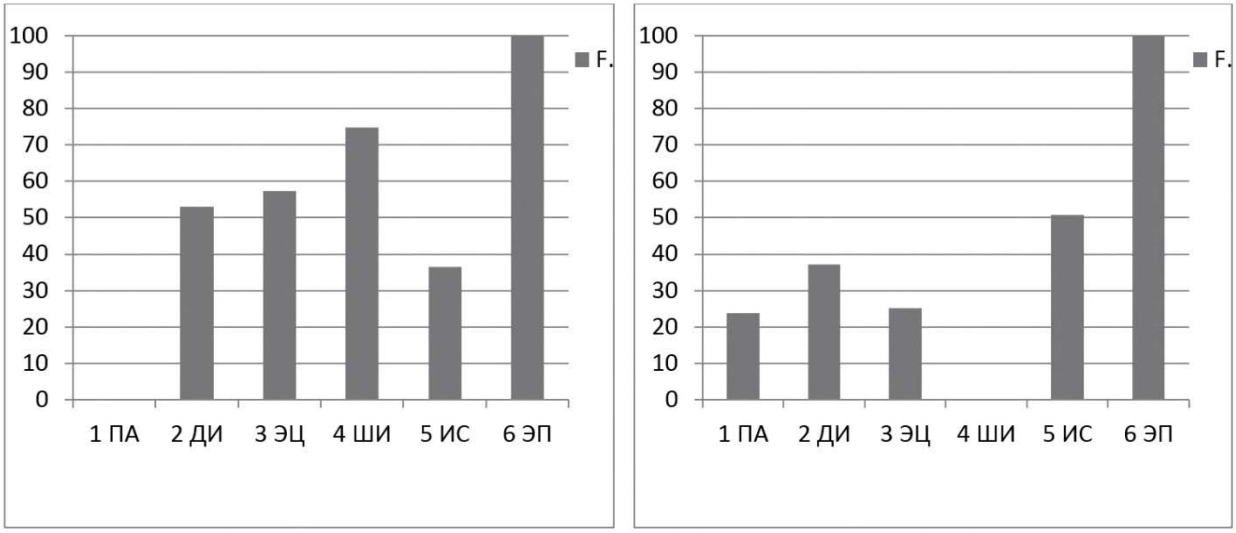
Согласно модели А.В. Гнездилова, совместимость и, следовательно, возможность продуктивного сотрудничества у пациентов и врачей, обладающих разными типами психологической акцентуации личностей, различаются. Так, например, пациент, принадлежащий к истероидной характерологической группе, скорее предпочтёт сотрудничать с врачом с шизоидной акцентуацией личности. Общение с доктором, обладающим таким же, как у него, психологическим профилем, будет крайне затруднительно.

Использование программы «PsyAccent» позволило получать данные о характере психологической акцентуации личности (6 основных типов) за несколько минут, в зависимости от когнитивных способностей испытуемого, и выявлять потенциальную совместимость личностей лечащего врача. Каждому испытуемому обследование проводилось однократно, в амбулаторном режиме или в условиях стационара. После обследования производили устный опрос пациента о его удовлетворённости работой лечащего врача. Ни один испытуемый не отметил неудобств и затруднений, связанных с компьютерным тестированием.

Результаты. Исследование показало возможность использования методики как на амбулаторном приёме, так и в условиях онкологического стационара.

Рассмотрим экспериментальные данные, полученные при помощи программы «PsyAccent».

В одном из наблюдений, результаты которого представлены на рис. 1, преобладание эпилептоидного типа психологической акцентуации и у врача М., и у пациента Ф. обусловило возникновение микро-конфликта уже на ранних этапах организации лечения. Больной проявил немотивированное недовольство и настаивал на замене лечащего врача, не отказываясь при этом от проведения обследования и лечения, назначенных этим доктором. По данным А.В. Гнездилова, крайне нежелательным является взаимодействие лечащего врача и больного с идентичными эпилептоидными типами психологической акцентуации (табл.1).

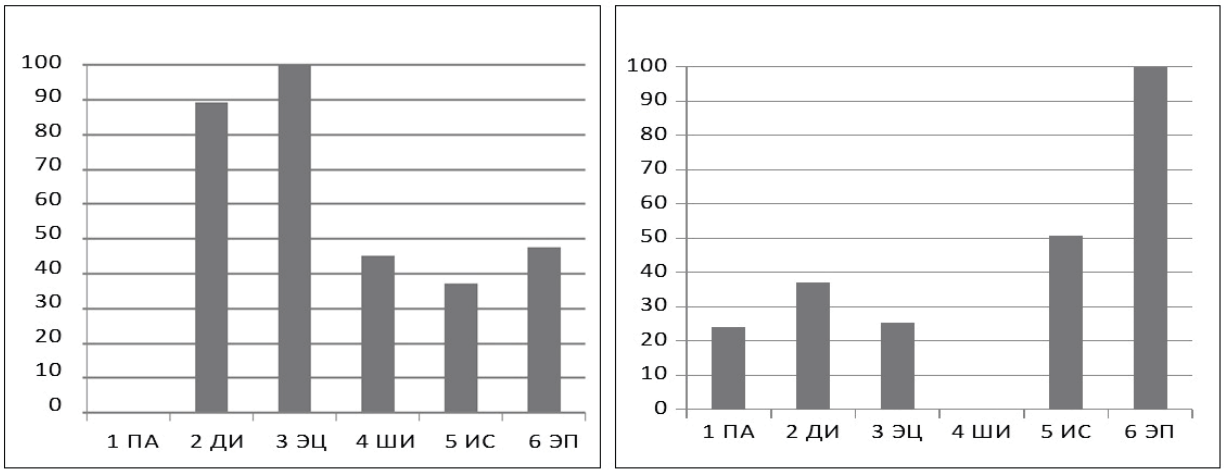


А) Б)

Рис. 1. Психологические профили пациента Ф. и врача М., полученные в результате обследования при помощи программы «PsyAccent».

А) пациент Ф., онкологический больной; Б) лечащий врач М. 1 ПА – психастенический тип психологической акцентуации личности (ТПАЛ), 2 ДИ – дистимический ТПАЛ, 3 ЭЦ - эмотивно-циклоидный ТПАЛ, 4 ШИ – шизоидный ТПАЛ, 5 ИС – истероидный ТПАЛ, 6 ЭП – эпилептоидный ТПАЛ

Другой пациент С. с преобладающей циклоидной и дистимной психологической акцентуацией был полностью удовлетворён работой того же самого врача М. и отмечал его высокий профессионализм и «прекрасные душевные качества». Психологические профили врача М. и пациента С. с преобладанием эпилептоидной и циклоидно-дистимной акцентуациями соответственно представлены на рис. 2.



А) Б)

Рис. 2. Психологические профили пациента С. и врача М., полученные в результате обследования при помощи программы «PsyAccent».

А) пациент С., с таким же диагнозом, как и больной Ф. из первой пары; Б) лечащий врач М. 1 ПА – психастенический тип психологической акцентуации личности, 2 ДИ – дистимический ТПАЛ, 3 ЭЦ - эмотивно-циклоидный ТПАЛ, 4 ШИ – шизоидный ТПАЛ, 5 ИС – истероидный ТПАЛ, 6 ЭП – эпилептоидный ТПАЛ

Малочисленность наблюдений не позволяет делать строго научные выводы о правильности созданной нами модификации модели, но отдельные наблюдения подтверждают правильность нашего выбора.

Заключение.

Проведённое тестирование в целом подтвердило необходимость продолжения исследований психологической совместимости лечащего врача и пациента как профилактической меры конфликтных

ситуаций. Использование методики «PsyAccent» позволяет быстро и комфортно для испытуемых проводить тестирование как в стационарных, так и в амбулаторных условиях, а также эффективно определять тип психологической акцентуации человека как фактора психологической совместимости пациента и врача, что необходимо для формирования позитивных взаимоотношений между ними. Мы полагаем, что возможности плодотворного использования программы «PsyAccent» выйдут далеко за пределы медицины и найдут своё место в широком круге иных профессий, требующих комфортного и эффективного сотрудничества и взаимопонимания.

Выводы:

1. Программа «PsyAccent» позволяет быстро устанавливать тип психологической акцентуации взрослого человека, не создавая никакого дискомфорта для испытуемого.

2. Программа может быть использована как в стационарных, так и в амбулаторных условиях.

3. В клинических условиях полученные сведения о типе акцентуации могут помочь избежать возникновения конфликтных ситуаций, обусловленных психологической несовместимостью больного и лечащего врача.

4. Программа «PsyAccent» может быть полезна для формирования малых групп, работающих в больших коллективах.

5. Программа вполне пригодна для решения качественных задач. Поиск возможности решения количественных задач возможен только при существенном увеличении числа наблюдений.

СПИСОК ЛИТЕРАТУРЫ

1. Мишин Ю.Б. Философия рака. Этиология, патогенез, лечение и профилактика: Заметки практикующего врача-онколога. Волгоград: Волгоградское научное издательство, 2005. 108 с.
2. Стуков А.Н., Гершанович М.Л., Бланк М.А., Бланк О.А., Цырлина Е.В., Филов В.А. Симптоматическая терапия в онкологии. / Под ред. М.Л.Гершановича и В.А.Филова. СПб: NIKA, 2007. 288 с.
3. Гнездилов А.В. Путь на Голгофу. СПб.: Фирма «КЛИНТ», 1995. 136 с.
4. Полонников Р.И. На пути к постижению сущности электрических проявлений сознания. СПб.: Издательство «Анатолия», 2007. 188 с.
5. Бизюк А.П., Вассерман Л.И., Иовлев Б.В. Применение интегративного теста тревожности. Методические рекомендации. СПб., 2003.
6. Минкин В.А. Виброизображение. Спб.: Реноме, 2007. 108 с.
7. Бланк М.А., Рудницкий С.Б., Бланк О.А., Вассерман Е.Л., Вильнер Г.А., Жвалевский О.А., Денисова Д.М., Ширяева О.А. К оценке психосоматического статуса человека // Материалы научной конференции «От лучей Рентгена – к инновациям XXI века: 90 лет со дня основания первого в мире рентгенорадиологического института (Российского научного центра радиологии и хирургических технологий)» (с участием специалистов стран ближнего и дальнего зарубежья) 8-10 октября 2008 г. Санкт-Петербург. С. 343.
8. Минкин В.А., Николаенко Я.Н. Виброизображение и множественный интеллект. СПб.: Реноме. 2017. 156 с.
9. Минкин В.А., Николаенко Н.Н. Применение технологии и системы виброизображения для анализа двигательной активности и исследования функционального состояния организма // Медицинская техника. 2008. № 4(42). С. 30-34.
10. Леонгард К. Акцентуированные личности. Киев, 1989. 375 с.
11. Личко А.Е. Типы акцентуаций характера и психопатий у подростков. М., 1999. 416 с.

УДК 004.42

КЛАСТЕРНЫЙ АНАЛИЗ СТОМАТОЛОГИЧЕСКИХ ДАННЫХ

Никонорова Маргарита Леонидовна
Первый Санкт-Петербургский государственный медицинский университет им. акад. И.П. Павлова
Льва Толстого ул., 6-8, Санкт-Петербург, 197022, Россия
e-mail: nikonorovaml@1spbgmu.ru

Аннотация. Методы и технологии анализа данных Data Mining позволяют выявить ряд скрытых закономерностей и связей между данными различного характера. В статье представлены результаты кластерного анализа стоматологических данных в программной среде R и в прикладной программе RM. Проведено сравнение полученных результатов, определено количество совпадений.

Ключевые слова: методы кластеризации; программная среда R; Rapid Miner; анализ слюны; стоматология.

CLUSTER ANALYSIS OF DENTAL DATA

Nikonorova Margarita
Department of Physics, Mathematics and Informatics. Pavlov First Saint Petersburg State Medical University
6-8 L'va Tolstogo Str,. St. Petersburg, 197022, Russia
e-mail: nikonorovaml@1spbgmu.ru

Abstract. Methods and technologies of data analysis of Data Mining let identify a number of hidden patterns and connections between data of various nature. The article presents the results of cluster analysis of dental data in the programs R and RM. The results are compared, the number of matches is determined.

Keywords: cluster analysis; program R; Rapid Miner; saliva analysis; dentistry

Современные информационные технологии в настоящее время охватывают все сферы медицины, начиная от диагностики и заканчивая организацией работы клиник, поликлиник и лечебно-профилактических учреждений. Использование информационных технологий позволяет сократить время на обработку и анализ

данных, при этом наиболее часто используются такие средства как компьютеры, мобильные телефоны и Интернет. Интернет объединяет различные информационные ресурсы и обеспечивает свободный доступ к ним любому пользователю, имеет мощные поисковые системы, которые позволяют при минимальных затратах времени и сил найти необходимую информацию. Так, при поиске методов диагностики общих заболеваний путем анализа морфо-функционального состава слюны найдено 38 тысяч результатов поисковой системой Yandex и 88,3 тысяч результатов поисковой системой Google.

Слюна играет не только важнейшую роль в поддержании физиологического равновесия различных процессов в эмали зубов, но и может служить источником информации об общем состоянии организма. Так, в состав слюны входят антитела, которые вырабатываются организмом для борьбы с вирусами и патогенными микроорганизмами, что позволяет определить различные заболевания на ранних стадиях и предупредить их развитие. Известные способы диагностики ряда заболеваний по исследованию ротовой жидкости: воспалительный процесс в органах дыхания (патент РФ 2140080, МПК G01N 33/487), хронический гастродуоденит и функциональная диспепсия у детей (патент РФ 2270610, МПК A61B 10/00, G01N 33/483), нарушение вегетативной регуляции сердечного ритма у детей с гастроэзофагеальной рефлюксной болезнью (патент 2517370), гипертоническая болезнь и сахарный диабет (патент 2407018). По ряду параметров ротовой жидкости возможно прогнозирование течения заболеваний, в частности, воспалительных заболеваний (патент РФ 2286572, МПК G01N 33/52); заболеваний, сопровождающихся нарушением микрофлоры полости рта (патент РФ 2229130, МПК G01N 33/48), развития одностороннего или двустороннего нефролитиаза (патент 2396913). Все эти способы позволяют диагностировать заболевание организма по ряду специфических параметров ротовой жидкости, что нередко требует разработки и внедрения новых методик анализов. При этом перечисленные способы не применимы для диагностики и профилактики заболеваний полости рта [3].

Рассмотрим в качестве исходных данных результаты исследования морфофункционального состава слюны 86 пациентов различных возрастных категорий. Все пациенты, выбранные репрезентативно, изначально составляли 4 группы:

1 группа – без патологических изменений состояния здоровья (*19 пациентов*),

2 группа – обладают патологией печени, цирроз (*7 человек*),

3 группа – заболевания желудочно-кишечного тракта (*8 пациентов*),

4 группа – диагностирована алкогольная зависимость (*52 человека*).

При обследовании пациентов:

– изучался белковый состав слюны,

– проводился анализ маркеров воспалительного процесса

– устанавливались индексы соматического состояния здоровья:индекс гигиены (ИГ) и индекс гингивита (РМА).

Интеллектуальный анализ данных – Data Mining позволяет проводить глубокое исследование и обнаруживать в данных ранее неизвестные, практически полезные и достаточно интерпретируемые связи [1]. Примеры применения Data Mining в медицине приведены в книге [2]. Инструменты кластерного анализа встроены во многие статистические пакеты, например, STATISTICA, SPSS.

В многомерной статистике кластерный анализ позволяет анализировать данные на основе расстояний. В качестве показателей расстояния используются Евклидово расстояние (геометрическое расстояние), расстояние Чебышева (различие 2х объектов по одной из координат), Хемминга (среднее разности по координатам) и Минковского (позволяет увеличить или уменьшить вес атрибутов, по которым отличаются объекты). Следует отметить, что кластерный анализ определяет «наиболее возможно значимое решение». Процесс разбиения набора объектов данных в подмножества является процессом кластеризации и каждое подмножество представляет собой кластер, в котором объекты похожи друг на друга, но не похожи на объекты в других кластерах. Разные методы кластеризации могут генерировать разные кластеры в одном наборе данных. Решение задачи кластеризации является неоднозначным, так как не существует однозначно наилучшего критерия качества кластеризации; число кластеров неизвестно заранее и устанавливается в соответствии с некоторым субъективным критерием.

В настоящее время известно около 100 алгоритмов кластеризации. Трудно обеспечить четкое разделение методов кластеризации, поскольку методы могут перекрываться и используемый метод кластеризации может иметь функции из нескольких категорий. Методы кластеризации можно классифицировать по следующим категориям [5]:

– *разбиения*: осуществляется одноуровневое разбиение на наборы данных, каждый объект принадлежит одной группе, используются эвристические методы.

– *иерархии:* могут быть восходящими и нисходящими, отсутствует комбинаторное число различных вариантов, невозможно исправить ошибочные слияния или расщепления.

– *плотности:* отфильтровывают выбросы, обнаруживают кластеры произвольной формы.

– *grid:* квантуют пространство объектов в конечное количество ячеек, которые образуют структуру сетки; имеют быстрое время обработки, не зависят от количества объектов, но зависят от размера сетки

Разбиение данных выполняется выбранным алгоритмом кластеризации и может привести к обнаружению ранее неизвестных групп внутри данных. *Алгоритм кластеризации* – это функция $\alpha: X \to Y$, которая любому объекту $x \in X$ ставит в соответствие метку кластера $y \in Y$. Множество меток Y в некоторых случаях известно заранее, однако, чаще ставится задача определить *оптимальное число кластеров*, с точки зрения того или иного критерия качества кластеризации.

Каждый метод кластеризации можно рассматривать как точный или приближенный алгоритм поиска оптимального значения некоторого функционала (F_0, F_l).

Среднее внутрикластерное расстояние должно быть, как можно меньше:

$$F_0 = \sum_{y \in Y} \frac{1}{|K_y|} \sum_{F_0 y_i = y} \rho^2(x_i, \mu_y) \to min \quad (1)$$

$$K_y = \{\{x_i \in X^l | y_i = y\}\} \quad (2)$$

где кластер с меткой y:

μ_y –центр кластеров,

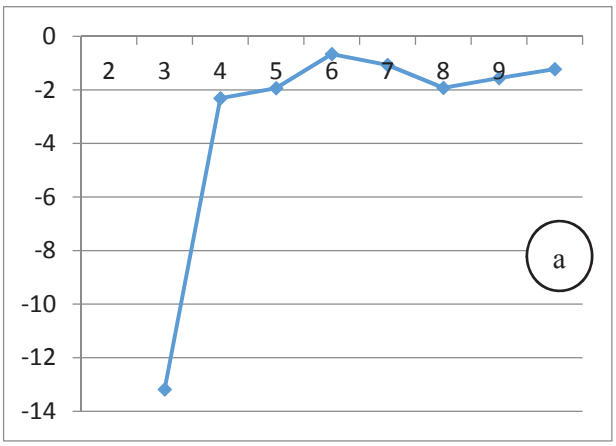
$|K_y|$ - число элементов в кластере

Среднее межкластерное расстояние должно быть как можно больше:

$$F_l = \sum_{yi \neq yj} \rho^2(\mu_{yi}, \mu_{yj}) \to max. \quad (3)$$

Алгоритмы кластеризации – неиерахического разделения (partitioning algorithms) выполняют поиск *центроидов* – максимально удаленных друг от друга центров кластера. К разделяющим алгоритмам относится метод *k* средних Мак-Кина (*k*-means clustering**,** MacQueen, 1967), который основан на расчете средневзвешенного расстояния в нормированном эвклидовом пространстве.

Для определения количества кластеров в исходной выборке можно воспользоваться «методом локтя» (Elbow Method), при котором выполняется кластеризация методом к-средних, рассчитывается и записывается значение функции (расстояние от объектов до центра). Кластеризация выполняется от 2 кластеров до $\sqrt{n}$, где n – количество объектов в выборке. Затем высчитывается разность между текущим и предыдущим значением функции и строится график зависимости функции от заданного числа кластеров, в качестве решения выбирается число кластеров. «Метод локтя» предполагает выбор в качестве оптимального значения k такую точку, где меняется характер поведения функции (рис.1, а). Очевидно, что при количестве кластеров k = 4 наблюдается наибольшее изменение функции, а далее характер поведения функции практически однороден. Можно отметить, что существуют и другие методики оценки числа кластеров: среднее расстояние между центрами кластеров (чем больше, тем лучше классификация) или алгоритм g-means, позволяет производить автоматический выбор оптимального числа кластеров на основании гауссовского (нормального) закона распределения. Наиболее просто определить число кластеров путем построения дендрограммы и отсечения её верхнего участка. Дендрограмма (dendrogram) - древовидная диаграмма, содержащая n уровней, каждый из которых соответствует одному из шагов процесса последовательного укрупнения кластеров. Пример построения дендрограммы в программе Rapid Miner приведен на рис. 1, б. Дендрограмму часто называют древовидной схемой, деревом объединения кластеров или деревом иерархической структуры. Определение числа кластеров производится путём отсечения верхнего участка дендрограммы: на вертикальной оси находится интервал максимальной длины, и линия отсечения проходит на уровне 4 кластеров, продвигаясь ниже происходит слияние ветвей дерева, то есть кластеры становятся похожи друг на друга. При необходимости можно задать ограничение на минимальное и максимальное число кластеров.



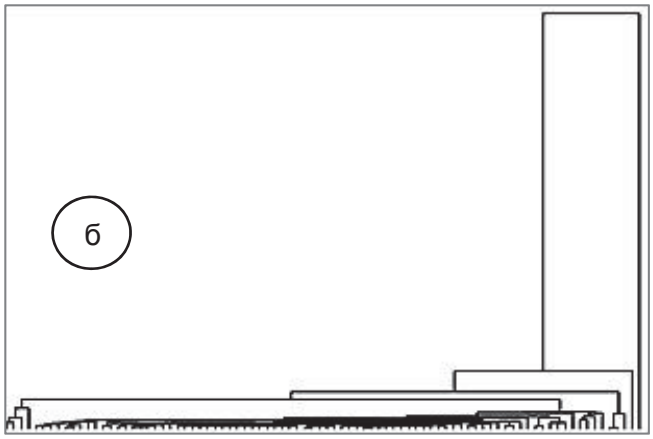


Рис.1. Метод локтя и дендрограмма кластеризации

Компьютерные средства обучения предоставляют большие возможности для анализа данных и значимой информации. Rapid Miner (RM) – бесплатное прикладное программное обеспечение, ориентированное на решение задач и построение модели принятия решений. Rapid Miner содержит более 500 операторов различных методов машинного обучения, включая ввод и вывод, предварительную обработку и визуализацию данных. Для

построения компьютерной модели кластеризации в RM необходимы операторы: Retrive, Normalize, Clustering (k-medoids) и Perfomance. Центр кластера, центроид, определяется как точка, для которой каждое значение атрибута является средним значением соответствующего атрибута для всех точек в кластере. Центроид кластера всегда будет одной из точек в кластере. Это основное различие между алгоритмом k-means и k- medoids, в алгоритме k-means центроид кластера часто бывает виртуальной точкой. Для построения дендрограммы используются операторы Retrive и Agglomerative Clustering.

Язык программирования R (программная среда R**)** широко используется как статистическое программное обеспечение для анализа данных и фактически стал стандартом для статистических программ**.** Код и результат кластерного анализа в программной среде R показан на рис. 2. Визуальное представление стоматологических данных по кластерам показано на рис. 3.

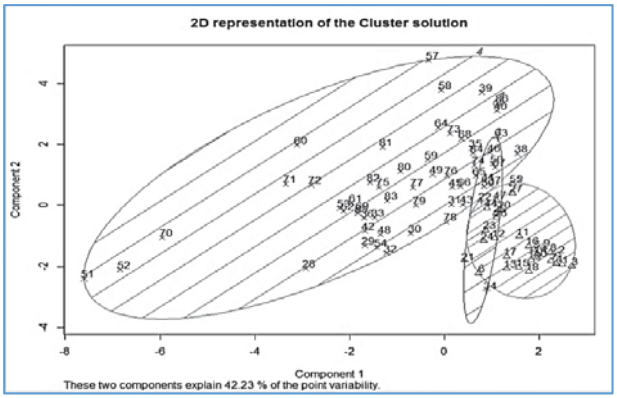
```
> res_stomat<-readxl::read_excel("I:/Stomat.xlsx")

> stomat.stand<-scale(res_stomat[-1])

> k.means.fit<-kmeans(stomat.stand,4)

> k.means.fit$size
```

Рис.2. Программный код и результат кластерного анализа




```
> cluster::clusplot(stomat.stand,k.means.fit$cluster,

+main='2D representation of the Cluster solution',

+ color=TRUE, shade=TRUE, labels=2,lines=0)
```

Рис. 3. Кластерное разделение стоматологических данных

Результаты проведенных исследований в программе RM и программной среде R приведены в таблице 1.

Таблица 1

Состав кластеров в RM и R

№ кластера	Количество пациентов, в том числе по группам									
	RM	R	группа 1		группа 2		группа 3		группа 4	
			RM	R	RM	R	RM	R	RM	R
0	12	4	8	–	1	2	1	1	2	1
1	54	53	4	–	3	–	7	6	40	47
2	1	1	–	–	–	–	–	–	1	1
3	19	28	7	19	3	5	–	1	9	3
ИТОГО:	86	86	19	19	7	7	8	8	52	52

Программой RM в сформированный кластер_0 отобраны 8 пациентов из 1 группы, по пациенту из 2 и 3 групп (2 человека), 2 пациента из 4 группы, то есть 12 пациентов. Программа R отнесла к кластеру_0 4 пациента: по одному из 3 и 4 группы, 2 пациента из 2 группы. Основу кластера_1 составляют пациенты 4 группы, а именно, 40 человек (RM) или 47 человек (R). Группа 3 в этом кластере представлена 7 пациентами (RM) или 6 пациентами (R). Также программой RM отнесены к кластеру_1 пациенты 1 группы (4 человека) и пациенты 2 группы (3 человека). Общее количество пациентов в кластере_1 почти совпадает: 54 человека (RM) и 53 человека (R). Кластер_2 сформированный в программе RM подобен кластеру в программе R. Принадлежность к кластеру_3 в программе RM отмечена у 19 пациентов, из них 7 пациентов 1 группы, 3 пациента 2 группы и 9 пациентов 4 группы. Программа R отметила 28 пациентов для кластера_3, это 19 пациентов 1 группы, 5 пациентов 2 группы, один пациент 3 группы и 3 пациента 4 группы.

Plot отличий кластеров, построенный в программе RM, показывает, что для пациентов, входящих в кластер_0, характерно высокое значение маркера воспаления; в кластере_1 значение PMA отличается от всех остальных, поэтому можно говорить об стоматологическом воспалении; пациент кластера_2 отличается повышенным врожденным иммунитетом; кластер_3 отличается от всего остального присутствием различных вирусных инфекций, в частности, выделено повышенное значение гамма интерферона.

После полученных результатов определяется количество совпадений объектов кластерного анализа в программных средах RM и R. Кластер_0 содержит 35% совпадений объектов; кластер_1 – 88%; кластер_2 – 100%; кластер_3 – 50% совпадений. Следовательно, можно предположить, что выявлен врожденный иммунитет, и пациенты с различными стадиями воспаления десен (индекс гингивита, PMA). Существует эмпирическое правило – устойчивая группировка должна сохраняться при изменении методов кластеризации: например, если результаты кластерного анализа имеют долю совпадений более 70% с группировкой по методу k средних, то предположение об устойчивости принимается. В программной среде R вычислено отношение суммы внутрикластерных расстояний к сумме межкластерных расстояний, оно составляет 28,9%, что считается признаком качественной кластеризации [4].

Вместе с тем, следует отметить, что кластерный анализ — это метод обучения без учителя, поэтому не существует правильных или неправильных результатов кластеризации. В большинстве случаев на практике поставленная задача сводится к приблизительной оценке, на сколько групп целесообразно разделить исходные данные. При этом большое достоинство кластерного анализа в том, что он позволяет производить разбиение объектов не по одному параметру, а по целому набору признаков. Кроме того, кластерный анализ в отличие от большинства математико-статистических методов не накладывает никаких ограничений на вид рассматриваемых объектов, и позволяет рассматривать множество исходных данных практически произвольной природы.

Сравнивая различные прикладные программы, используемые для проведения кластеризации можно отметить вариативность, гибкость и универсальность программной среды R; наглядность и визуализацию, дружественный интерфейс программы Rapid Miner. Полученные результаты кластерного анализа позволяют сформировать решение, обобщить собранные данные и разработать соответствующие рекомендации.

СПИСОК ЛИТЕРАТУРЫ

1. Дюк В., Самойленко Л. Data Mining: учебный курс. – СПб: Изд. Питер, 2001. – 368 с.
2. Дюк В., Эммануэль В. Информационные технологии в медико-биологических исследованиях. – СПб.: Питер, 2003. – 528 с.
3. Патентный поиск в РФ.: [Электронный ресурс] //Новые патенты, заявки на патент. Библиотека патентов на изобретения. – Режим доступа: http://www.freepatent.ru/patents/2367959.
4. Шитиков В.К. Мастицкий С.Э. Классификация, регрессия и другие алгоритмы Data Mining с использованием R. [Электронный ресурс] / Шитиков В.К. Мастицкий С.Э. 2017. – 351 с. – Режим доступа: https://github.com/ranalytics/data-mining.
5. Jiawei Han, Micheline Kamber, Jian Pei. Data mining : concepts and techniques / Jiawei Han, Micheline Kamber, Jian Pei. – 3rd ed. – ELSEVIER, 2012. –703 p.

УДК 004.051:61

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В МЕДИЦИНЕ

Шугай Антон Андреевич
Исследовательская блокчейн-лаборатория brdt.pro
Набережная Адмиралтейского канала, 2Т, офис 403, Санкт-Петербург, 190098, Россия.
e-mail: anton@brdt.pro

Аннотация. В статье рассматриваются сценарии применения технологии блокчейн в медицинской отрасли на примере существующих проектов, описываются проблемы внедрения технологии и преимущества, которые она даст после масштабного внедрения. Было проведено исследование существующих проектов как в России, так и в мире. Выявлены наиболее популярные направления, в которых ведется активная разработка решений на основе технологий распределенного реестра.

Ключевые слова: блокчейн; технологии распределенного реестра; медицина; отслеживание происхождения; хранение и управление данными; телемедицина; диагностика; привлечения средств.

BLOCKCHAIN IN MEDICINE: USE CASES OF TECHNOLOGY

Shugai Anton
Blockchain research laboratory brdt.pro
2T Naberegnaja Admiralteiskogo kanala, off. 403, St. Petersburg, 190098, Russia
e-mail: anton@brdt.pro

Abstract. The report on projects that claim the use of blockchain technologies in healthcare. A case study was conducted among existing projects. The most popular trends of distributed ledger technologies application were identified.

Keywords: blockchain; distributed ledger technology; medicine; logistics; data storage and management; telemedicine; diagnostics; fundraising.

Согласно исследованию Delloite 2018 Global Health Care Outlook затраты на здравоохранение в мире к 2020 году составят 8,7 триллионов долларов.

Между тем, в отрасли сформировались и оказывают значительное влияние на величину издержек следующие проблемы:

1. Контроль оборота рецептурных препаратов.
2. Фальсификация медикаментов: в аптечные сети попадают поддельные медицинские препараты, которые в лучшем случае не вызывают никакого эффекта (плацебо), а в худшем - влияют на здоровье пациентов.
3. Отсутствие единой системы хранения медицинских данных пациентов: медицинские ошибки - одна из основных причин смертности в США и по мнению экспертов [10] эти ошибки могут бытьт вызваны отсутствием единой системы хранения и передачи данных. Эта проблема зафиксирована не только в США - разнообразие информационных систем порождает несовместимость данных и, как следствие, наносит вред пациентам.
4. Клинические испытания: данные по клиническим испытаниям зачастую непрозрачны и не общедоступны.
5. Большие затраты на поддержание информационных систем: поскольку для каждого процесса запускают свою ИС, то их совокупное содержание начинает стоить очень дорого.

Все эти проблемы в общем сводятся к одной общей большой проблеме: обеспечение целостности, совместимости, доступности, актуальности и прозрачности информации в системе здравоохранения.

Если отдельно рассмотреть вопрос совместимости данных, то можно обратить внимание, что долгое время внимание уделялось только взаимодействию организаций («система-система»). Однако в последнее время наблюдается смещение фокуса в сторону взаимодействия «пациент-система», когда пациент самостоятельно контролирует свои медицинские данные. Такой подход поднимает совершенно новый пласт проблем, связанных с приватностью и безопасностью данных, а также их управлением. По мнению экспертов [4, 8] именно блокчейн сделает возможным переход от типа взаимодействия “система-система” к “пациент-система” за счет своих уникальных качеств.

Таким образом, сфера здравоохранения давно нуждается в изменениях и сегодня есть множество возможностей для технологии blockchain возглавить трансформацию. Интерес к самой технологии стал заметен в последний год, в том числе и в сфере здравоохранения. Доказательством возросшей востребованности технологии blockchain могут служить результаты исследования, проведенного в октябре 2017 года командой «Black Book Market Research» [1]. В нем было опрошено 88 потребителей системы здравоохранения (среди них, представители страховых компаний, потребители медицинских услуг) и 276 поставщиков медицинских услуг (отвечающих за технологических процесс специалистов, менеджеров и IT-специалистов).

Опрос выявил, что 19% управляющих медицинскими организациями и 76% представителей, оплачивающих медицинские услуги, рассматривали или уже применяли решения на основе технологии blockchain. 70% организаций, оплачивающих медицинские услуги, ожидают интеграцию blockchain в существующие системы и 9% поставщиков медицинских услуг собираются использовать новую технологию уже в 2018 году.

В 2018 году подобное исследование провела компания Deloitte [3]. Исследователи опрашивали исполнительных директоров разнообразных медицинских учреждений и выяснили, что 55% опрошенных считают блокчейн эволюционным прорывом, 60% согласны, что если не внедрять блокчейн-технологии, то можно потерять конкурентное преимущество и 63% сказали, что их компании планируют инвестировать не менее 1 миллиона долларов во внедрение блокчейна.

Таким образом, повышенное внимание к технологии распределенных реестров привело к пониманию потенциала их применения в системе здравоохранения. Эти обстоятельства дали благодатную почву для команд и организаций, желающих интегрировать технологию blockchain в уже существующие проекты или разработать новые, отвечающие требованиям высоких технологий и работы с большим объемом данных.

Технология блокчейн это по сути распределенная база данных, обладающая такими свойствами как прозрачность, неизменяемость и формирование доверенной среды передачи данных. Технология обычно внедряется вместе со своим следующим слоем - смарт-контрактами, которые обеспечивают автоматизацию исполнения, гарантируют отсутствие двусмысленных трактовок и исключают необходимость посредников. Запись информации в блокчейн происходит на базе консенсуса между пользователями сети, что позволяет определить четкий алгоритм определения истины и принятия решений, тем самым добавляя такие свойства как объективность и прозрачность информации.

Поскольку, как мы уже упомянули, основная проблема в здравоохранении связана с областью работы с информацией, вышеперечисленные свойства и качества блокчейна позволяют оптимизировать информационный обмен, а также определить объективность, прозрачность и достоверность данных.

Сама сущность блокчейна - распределенная база данных - решает проблему хранения информации. Смарт-контракты автоматизируют обмен данными между медицинскими учреждениями, а также позволяют непосредственно пациентам передавать свои данные компаниям и получать за это вознаграждение; кроме того смарт-контракты гарантируют безопасность и сохранение приватности этих данных. А четко формализованные методы консенсуса обеспечат прозрачность и объективность медицинских данных.

Области, в которых внедрение блокчейна будет максимально полезным [2]:

1. Клинические испытания: хранение данных, гарантия их неизменяемости и прозрачности [7].
2. Нормативно-правовое соответствие: регистрация согласия пациента, обмен медицинскими данными
3. Отслеживание оборота медицинских средств: фиксация перемещений меток (например, RFID) и условий хранения медицинских препаратов. Выявление контрафакта.

4. Платежи и сопровождение рекламации: любые финансовые и страховые операции, фиксация и контроль исполнения по претензиям.

Несмотря на всю перспективность применения блокчейна в здравоохранении, технология также сталкивается с некоторыми проблемами:

1. Масштабируемость.
2. Скорость.
3. Размер базы.
4. Алгоритмы консенсуса.
5. Стандарты и законодательство.

Проблемы эти решаются (и многие - например, проблема скорости и масштабирования уже практически решены) и не мешают разработчикам сформировать концепты уже сейчас, чтобы потом иметь возможность первыми применить их во всей отрасли. Когда технологические преграды будут устранены, начнется массовое внедрение технологии во всей отрасли.

Видят перспективы технологии и российские чиновники:

6 сентября 2017 года министр здравоохранения РФ Вероника Скворцова так описала грядущую цифровизацию системы хранения медицинских данных:

«Система [хранения электронных медицинских карт] будет устроена по принципу блокчейн. Она будет деперсонализирована, что позволит эти данные сохранить в полной безопасности. Ключ будет индивидуализированный».

25 мая 2018 года губернатор Московской области Андрей Воробьев сказал:

«В Московской области планируется внедрить блокчейн в систему здравоохранения. В частности, новая технология может быть применена в электронных медицинских картах пациентов».

Также 20 октября 2018 года советник председателя правления ВЭБа Владимир Демин рассказал про ход пилотного проекта по внедрению блокчейна в систему контроля оборота медицинских препаратов в Новгородских клиниках:

«В ходе пилотного проекта [в Новгородской областной клинической больнице] мы запатентовали несколько технологический решений, что позволит в перспективе транслировать их как в иные проекты в этой сфере [в сфере блокчейн], так и в систему лекарственного обеспечения всей страны».

Стоит понимать, что вместо “изобретения велосипеда”, иногда эффективнее присоединиться к существующему проекту и адаптировать его под локальный рынок. Тем более, что сама технология blockchain является международной и децентрализованной. В этом смысле, наше стремление сделать свой российский продукт просто не актуально. 99% проектов имеют полностью открытый код и зачастую готовы финансировать разработку сторонними командами.

В силу новизны блокчейн-технологии и, следовательно, отсутствия давно работающих в сфере здравоохранения проектов, пока не существует четкого представления о временных рамках внедрения и оценки его эффективности: пока что исследователи имеют дело с пилотными проектами и уже стало ясно, что основные сложности лежат не в поле собственно внедрения, а в области изменения существующих парадигм и процессов, культурных и бизнес-«привычек» в сфере здравоохранения [9]. Технологии еще только предстоит доказать свою эффективность и способность масштабироваться на всех участников процесса (как организаций, так и пациентов).

Ниже мы рассмотрим, какие проекты уже существуют на стыке медицины и технологии blockchain. Какие из них работают, а какие находятся лишь на стадии прототипа или идеи. Для этого, лаборатория brdt.pro провела исследование проектов в сфере здравоохранения, заявляющих о применении технологии блокчейн. В рамках этого исследования были рассмотрены их цели, задачи, и пути решения выявленных проблем.

Свойства блокчейна, которые используются как основной аргумент для необходимости его внедрения: прозрачность, доверительная среда, гарантия неизменяемости данных, наличие механизмов, обеспечивающих их совместимость, приватность и безопасность. Каждый рассмотренный проект использует несколько свойств из этого списка.

Рассмотренный проекты можно разделить на несколько направлений.

1) Отслеживание происхождения: актуально и востребовано использование распределенного реестра для регулирования фармацевтических поставок и отслеживания медикаментов [5]. Разработка платформ, к которым будут иметь доступ как поставщики услуг, так и контролирующие органы, поможет наладить прозрачные партнерские отношения и избежать мошенничества.

Какие свойства блокчейна важны: прозрачность и неизменяемость данных, доверительная среда.

Примером внедрения можно назвать пилотный проект «Блокчейн в системе льготного лекарственного обеспечения» в Новгородской области. Цель проекта: контроль процесса лекарственного обеспечения отделений больницы и льготного лекарственного обеспечения пациентов с рассеянным склерозом. Что уже сделано: подключено 3 отделения больницы, сейчас идет стадия подключения амбулаторного отделения.

Также можно отметить успехи проекта MediLedger - открытой сети на основе блокчейн для урегулирования поставки фармацевтических препаратов. В октябре 2018 уже запускается сервис по проверке идентификатора продукта, что соответствует требованиям законодательства США (к 27 ноября 2019 года все рецептурные препараты должны иметь уникальные идентификаторы).

2) Хранение и управление данными [6, 8]: разработка систем для хранения личных медицинских записей на основе blockchain. Продуктом является удобный интерфейс для пациента, отражающий всю информацию по здоровью и медицинские записи. К платформе также получают доступ поставщики медицинских услуг,

фармацевтические компании, страховые компании и исследовательские организации. Представленная в виде графиков информация о здоровье пациентов, к которой они сами могут открыть доступ и получить за это деньги от исследовательских организаций, поможет специалистам улучшить методики лечения, привлечь клиентов, увеличить прибыль, избежать различных издержек, при этом сокращая расходы на административный ресурс. Это одно из самых популярных направлений.

Какие свойства блокчейна важны: на первое место выходят механизмы, обеспечивающие совместимость, приватность и безопасность данных.

Здесь можно упомянуть британский проект Medicalchain, который проводит пилотный проект совместно с The Groves Medical Group (Медицинский центр, Великобритания) с июля 2018. Они гарантируют полный доступ и контроль данных, получение онлайн консультаций у специалистов, а также возможность продажи данных фармацевтическим компаниям для проведения исследований.

Инициатива e-Health в Эстонии - объединенный проект Фонда электронного здравоохранения Эстонии и компании Guardtime по созданию единой базы медицинских карт на блокчейне. Технология, которую применяют в рамках работы очень похожа на блокчейн, хотя и была создана еще до того, как этот термин вошел в обиход.

Не отстает и Австралия - государственная платформа My Health Record провела пилотное внедрение блокчейна. Основная цель: защита данных пациентов, обмен данными между исследователями. Пилотный проект выявил, что перед полномасштабным внедрением данные на платформе необходимо стандартизировать. Внедрение блокчейна планируется к 2020 году.

3) Взаимодействие между контрагентами.

Какие свойства блокчейна важны: прозрачность, доверительная среда, неизменяемость данных, а также их совместимость.

Два крупных консорциума - в Америке и в Европе запустили масштабные проекты, область задач которых сосредоточена на проблемах взаимодействий между различными агентами.

Пилотный проект в Америке запущен в апреле 2018 года, разработкой занимаются 5 организаций. Основная проблема, которую они решают - сокращение административных издержек страховщиков.

Блокчейн-проект в Европе My Health, My Data (объединение из 15 организаций). Их область деятельности - управление медицинскими данными (единая система хранения, обмен, безопасность).

Многие проекты, ведущие разработку в области новейших технологий, направленных на выявление болезней видят использование blockchain как маркетинговую кампанию по привлечению средств.

Заключение

Сегодня рано говорить о безусловной эффективности применения технологий распределенных реестров, однако уже отмечено, что технология, меняя принципы взаимодействия участников сложившейся экосистемы, создает возможность, к примеру, значительно снизить транзакционные издержки (такой же эффект отмечается не только в сфере здравоохранения но и в банковской системе). Процесс перехода будет не быстрым, так как он затрагивает множество независимых друг от друга организаций - как в коммерческом, так и в государственном секторе. Следовательно, такие изменения могут быть реализованы только в рамках консорциумов, ассоциаций или иных объединений и мы уже наблюдаем их формирование. По мнению многих экспертов, именно те организации, которые смогут первыми внедрить единые стандарты взаимодействия на базе технологий распределенных реестров, будут лидерами будущей медицинской отрасли.

СПИСОК ЛИТЕРАТУРЫ

1. Healthcare Industry interest in Blockchain is heating up, Black Book Survey, Q3, 2017/ [Электронный ресурс] URL: https://www.newswire.com/files/16/40/321b6089f1b01dfd80433bffb0df.pdf (дата обращения 28.02.2018)
2. Bresnik J., Five Blockchain Use Cases for Healthcare Payers, Providers, 2017. [Электронный ресурс] URL: https://healthitanalytics.com/news/five-blockchain-use-cases-for-healthcare-payers-providers (дата обращения 28.02.2018)
3. Deloitte 2018 Global health care outlook: The evolution of smart health care, 2018. [Электронный ресурс] URL: https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/global-health-care-sector-outlook.html (дата обращения 28.02.2018)
4. William J.Gordon, Christian Catalini. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Computational and Structural Biotechnology Journal Volume 16, 2018, Pages 224-230 [Электронный ресурс] URL: https://www.sciencedirect.com/science/article/pii/S200103701830028X (дата обращения 05.12.2018)
5. Koshechkin K.A., Klimenko G.S, Ryabkov I.V., Kozhin P.B. Scope for the Application of Blockchain in the Public Healthcare of the Russian Federation. Procedia Computer Science 126 (2018) 1323–1328 [Электронный ресурс] URL: https://www.sciencedirect.com/science/article/pii/S1877050918313607 (дата обращения 05.12.2018)
6. Ahmed F. Husseina, ArunKumar, GustavoRamirez-Gonzalez, Enas Abdulhay, João Manuel R.S. Tavares, Victor Hugo C.de Albuquerque. A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform. Cognitive Systems Research Volume 52, December 2018, Pages 1-11 [Электронный ресурс] URL: https://www.sciencedirect.com/science/article/pii/S1389041718301177 (дата обращения 05.12.2018)
7. Athina-Styliani Kleinaki, Petros Mytis-Gkometh, George Drosatos, Pavlos S. Efraimidis, Eleni Kaldoudi. A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval. Computational and Structural Biotechnology Journal Volume 16, 2018, Pages 288-297 [Электронный ресурс] URL: https://www.sciencedirect.com/science/article/pii/S2001037018300400 (дата обращения 05.12.2018)
8. James Brogan, Immanuel Baskaran, Navin Ramachandran. Authenticating Health Activity Data Using Distributed Ledger Technologies. Computational and Structural Biotechnology Journal Volume 16, 2018, Pages 257-266 [Электронный ресурс] URL: https://www.sciencedirect.com/science/article/pii/S2001037018300345 (дата обращения 05.12.2018)
9. How Will Blockchain Impact Healthcare? Tech Leaders Weigh In [Электронный ресурс] URL: https://healthtechmagazine.net/article/2018/08/how-will-blockchain-impact-healthcare-tech-leaders-weigh (дата обращения 05.12.2018)
10. Is the Technology Gap the Reason Why Medical Errors are the 3rd Leading Cause of Death in the US? 2016 [Электронный ресурс] URL: http://www.openhealthnews.com/articles/2016/technology-gap-reason-why-medical-errors-are-3rd-leading-cause-death-us (дата обращения 05.12.2018)

http://spoisu.ru

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

УДК 681.3.06

ПРИНЦИПЫ АВТОМАТИЗАЦИИ ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ ОБРАЗОВАТЕЛЬНЫМИ СИСТЕМАМИ ПО ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО УПРАВЛЕНИЮ ОБЪЕКТАМИ МОРСКОЙ ИНФРАСТРУКТУРЫ

Алексеев Сергей Алексеевич, Парфенов Николай Петрович, Стахно Роман Евгеньевич, Яковлева Наталья Александровна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: ksgati@yandex.ru

Аннотация. Установлено, что повышение эффективности организационного управления образовательных систем сопряжено с созданием и внедрением в процесс подготовки будущих специалистов по управлению объектами морской инфраструктуры различного рода автоматизированных систем. Достижение целей автоматизации систем организационного управления образовательных систем должно базироваться на соблюдении двух групп принципов: организационных и технических. Определен перечень видов технологий реализации способов организационного управления образовательных систем с использованием комплекса средств автоматизации в зависимости от организационной структуры образовательной системы, числа обучающихся и требуемого уровня формирования умений и навыков.

Ключевые слова: эффективность; организационное управление; образовательная система; комплекс средств автоматизации.

PRINCIPLES OF AUTOMATION IN ORGANIZATIONAL MANAGEMENT OF EDUCATIONAL SYSTEMS FOR TRAINING SPECIALISTS IN MANAGEMENT OF OBJECTS OF THE MARITIME INFRASTRUCTURE

Alekseev Sergey, Parfenov Nikolay, Sakhno Roman, Yakovleva Natalia
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St., St. Petersburg, 198206, Russia
e-mail: ksgati@yandex.ru

Abstract. It is established that increasing the efficiency of organizational management of educational systems is associated with the creation and implementation in the process of training of future specialists in the management of marine infrastructure of various kinds of automated systems. Achieving the goals of automation of organizational management systems of educational systems should be based on compliance with two groups of principles: organizational and technical. The list of types of technologies for the implementation of methods of organizational management of educational systems using a complex of automation depending on the organizational structure of the educational system, the number of students and the required level of skills.

Keywords: efficiency; organizational management; educational system; complex automation.

Введение.

Объективно существует противоречие между сложностью задач по организационного управления (ОУ) и неразвитостью имеющихся у руководителей образовательных систем (ОС)методов и средств в принятии решений. Преодолению этого противоречия способствует применение средств автоматизации на всех уровнях ОУ подготовкой специалистов по управлению объектами морской инфраструктуры. Использование ЭВМ, АСУ, автоматизированных систем поддержки принятия решения (АС ППР), экспертных систем (ЭС) может создать принципиально новую ситуацию в предметной области ОУ ОС. При этом необходимо использовать результаты исследования человеко-машинных технологий управления, современных информационных технологий, включающие методы и процедуры сбора, накопления, передачи, хранения и выдачи информации пользователям (руководителю ОС и обучающимся) в удобном для них виде, а также, приемы работы с техническими устройствами и ПЭВМ.

На сегодня возможны различные модификации АС ППР, которые могут использоваться в ходе управления ОС:

1) информационные, обеспечивающие лицо, принимающего решение (ЛПР) (руководителя ОС) своевременной, релевантной и точной информацией на всех этапах процесса управления ОС;

2) вычислительные, осуществляющие анализ и обработку информации об управляемом объекте системы ОС по заданным алгоритмам;

3) информационно-вычислительные, представляющие собой симбиоз двух названных систем;

4) интеллектуальные, основанные на использовании баз знаний (БЗ) и методов ИИ.

АС ППР любого класса для использования в контуре ОУ ОС должны обладать средствами максимально дружественного диалога с руководителем ОС. При этом должна широко использоваться БЗ руководителя ОС о его предметной области, а также информация о его личном опыте по ОУ ОС (функция ЭС), включающая графическую, понятийную информацию, как дополнение к фактографической и документальной информации сопровождения технических систем (ТС).

Применение в контуре ОУ ОС любой из названных систем (АСУ, АС ППР, ЭС) должно обеспечивать целенаправленное управление качественными характеристиками ОС, т.е. ее содержанием, деятельностью руководителей ОС и обучающихся, методами, средствами и организационными формами ОС. Для реализации ОУ ОС только при широком использовании средств автоматизации реально обеспечить возможность оперировать со всеми моделями организационной и дидактической подсистем ОУ ОС одновременно.

Достижение стоящих перед автоматизированной системой (АС) ОУ ОС целей возможно только при условии, что ее разработка, внедрение и функционирование ориентированы на соблюдение основных принципов двух групп: организационных и технических. Перечень и содержание основных организационных принципов создания, внедрения и функционирования АС ОУ ОС показаны в таблице 1, а перечень технических принципов разработки, внедрения и эксплуатации названной системы в таблице 2.

Таблица 1

Организационные принципы создания, внедрения и функционирования АС ОУ ОС

Организационный принцип	Содержание организационного принципа
Системности	Разработка, внедрение и функционирование АС ОУ ОС должны вестись на основе глубокого анализа системы ОС как педагогической системы, процессы управления качественными характеристиками которой подлежат автоматизации, на четком определении взаимосвязанных задач ее разработки, внедрения и функционирования.
Соответствия	Выделение на основе анализа основных функций АС ОУ ОС, реализуемых в процессе ОС, соответствующих им задач ОУ ОС, которые ранее решались не в полном объеме или не решались совсем.
Целесообразности	В контуре АС ОУ ОС должны решаться те и только те задачи, для которых может быть получен положительный эффект от их автоматизации, т.е. выигрыш от экономического, педагогического, социального эффекта должен превышать затраты.
Психологичности	Преодоление негативных явлений, возникающих при внедрении в практику ОУ ОС средств автоматизации, что связано с психологическими особенностями коллектива руководителей ОС и управленческого персонала (отказ от привычных способов управления ОС, слабая компьютерная подготовка, утрата статуса, нарушение сложившегося стереотипа мышления).
Непрерывности	Обеспечение оперативного изменения функций АС ОУ ОС, адаптации всех видов ее обеспечения к изменяющимся условиям реализации процесса ОС.

Таблица 2

Технические принципы, разработки, внедрения и эксплуатации АС ОУ ОС

Технический принцип	Содержание технического принципа
Типизации и унификации	Разработка АС ОУ ОС должна вестись на основе ГОСТ, пакетов прикладных программ, параметрически настраиваемых на конкретные условия, типовых и унифицированных средств автоматизации и вычислительной техники, единой системы технологических операций, кодирования, правил эксплуатации подсистем и их классификации.
Сбалансированности	Проектные решения ввода, обработки, хранения и обмена информацией между подсистемами АС ОУ ОС должны обеспечивать баланс между минимизацией затрат на реализацию информационных процессов и максимизацией эффективности их использования подсистемами.
Гибкости	Проектирование информационных процессов, реализуемых в АС ОУ ОС должно обеспечивать выбор такой системы управления базами данных (СУБД), которая при необходимости позволяла бы реорганизовать

	логическую структуру БД без существенных трудозатрат с помощью утилит СУБД. Файлы БД должны быть организованы так, чтобы при минимальном их количестве хранящаяся в них информация, будучи уникальной, обеспечивала потребности подсистем АС ОУ ОС.
Согласованности	Проектные решения по информационному и программному обеспечению автоматизированной СОУ ОС должны незамедлительно внедряться в имеющиеся аппаратные средства системы, предусматривая возможность ее совершенствования по мере развития информационных, программных и аппаратных средств.
Модульности	Проектирование АС ОУ ОС целесообразно вести на основе функционально независимых модулей, что должно обеспечить исключение одних, модернизацию оставшихся и ввод новых с наименьшими трудозатратами.
Приемлемости	Необходимость принимать такие проектные решения при разработке, создании и внедрении АС ОУ ОС, в результате которых трудоемкость обслуживания системы соответствовала бы возможностям персонала работающего с ней.

Учет всех приведенных принципов автоматизации процессов ОУ ОС необходим, чтобы разрабатываемые и внедряемые в образовательный процесс автоматизированные организационные и дидактические подсистемы СОУ ОС оказались результативными, оперативными и малоресурсозатратными.

Фактически внедрение АС ОУ ОС эквивалентно новой технологии функционирования педагогической системы ОС, что потребует перестройки как структуры ОУ ОС, так и определенной корректуры оргштатной структуры.

При проектировании, внедрении и эксплуатации АС ОУ ОС необходимо учитывать ряд их принципиальных особенностей [1 - 4]:

Автоматизированные системы ОУ ОС носят явный человеко-машинный характер, т.е. являются системами «человек-машина». Поэтому при их проектировании, внедрении и эксплуатации необходимо использовать аппарат эргономики и инженерной психологии и развитые в этих научных направлениях методы, средства и формы учета их норм и требований в ходе эргономического обеспечения проектирования, экспертизы и эксплуатации названных систем.

Экспертиза адекватности принимаемых проектных эргономических (инженерно-психологических), технических, технологических и экономических решений при разработке такого класса сложных социальных организационно-технических систем должна проводиться на всех стадиях разработки экспериментальными, аналитическими методами и методами статистического и имитационного моделирования.

Автоматизированная система ОУ ОС может разрабатываться и внедряться (вводиться в эксплуатацию) отдельными частями, каждая из которых решает относительно самостоятельные задачи. При этом эксплуатация частей первой очереди сопровождается разработкой и внедрением последующих очередей, что требует четкого взаимодействия Заказчика и Разработчика системы.

Поскольку высшие учебные заведения особенно инженерно-технического профиля, располагают научными, педагогическими кадрами, способными решить задачу разработки, внедрения и эксплуатации АС ОУ ОС при соответствующем финансировании, то привлечение специализированных проектных организаций может оказаться нецелесообразным. Следовательно, в ряде случаев в процессе проектирования названных систем Заказчик выступает и в роли Разработчика, что позволяет сделать систему максимально адаптированной к условиям учебного заведения, к реализации процесса ОС и к потенциальным пользователям.

Человеко-машинный характер, сложность, наличие двухуровневости (руководитель ОС - обучающийся) и другие, уже перечисленные особенности АС ОУ ОС определяют сложность процедуры оценивания ее экономических показателей, т.к. оценивать следует экономичность эффективности практической (тренажерной) подготовки специалистов-выпускников учебного заведения. Полученная оценка эффективности зависит от очень большого числа разнородных и часто случайных факторов и к тому же проявляется через длительный промежуток времени (отзывы на выпускников с места службы должны поступать ежегодно в течение 5 лет).

Для повышения эффективности ОУ ОС по подготовке специалистов по управлению объектами морской инфраструктуры, необходимо осуществлять автоматизацию управления, базируясь на организационных и технических принципах с учетом особенностей АС ОУ ОС. Решение этой задачи должно обеспечить достижение целей каждого из мероприятий ОС, а также тех из них, которые определяют уровень достижения целей ОС в целом. Эффективное использование комплекса средств автоматизации (КСА) для достижения названных целей ОС базируется на соблюдении технологии психолого-педагогического проектирования АС ОУ ОС и использовании наиболее эффективных способов ОУ ОС. В связи со сказанным целесообразно разделение способов ОУ ОС, реализуемых с использованием КСА, на 4 группы (таблица 3). Ранги (номера) групп, к которым отнесены способы ОУ ОС, включающие технологии, использующие КСА, определяют последовательность (срочность) внедрения автоматизации управления, а сами технологии в соответствующих группах – целесообразность автоматизации соответствующих функций управления [1 - 3].

Таблица 3

Группы внедрения способов ОУ ОС с использованием технологий, включающих КСА

№ группы	Вид способов ОУ ОС	Степень обязательности внедрения
1	Способы, достижение целей которых не обеспечивается на основе применяемой неавтоматизированной технологии ОУ ОС, но обеспечивается на основе новой технологии, использующей КСА	Обязательная в настоящий момент
2	Способы, достижение целей которых оказывает определяющее положительное влияние на уровень практической подготовки и частично обеспечивается использованием неавтоматизированной технологии ОУ ОС, но может быть существенно повышено на основе новой технологии, использующей КСА	Первоочередная
3	Способы, достижение целей которых оказывает некоторое общее положительное влияние на уровень практической подготовки и частично обеспечивается использованием неавтоматизированной технологии ОУ ОС, но может быть повышено на основе новой технологии, использующей КСА	Периодическая
4	Способы, достижение целей которых оказывает некоторое частное положительное влияние на уровень практической подготовки и обеспечивается в целом использованием неавтоматизированной технологии ОУ ОС, но внедрение в нее элементов новой технологии, использующей КСА, может несколько повысить эффективность управления	Эпизодическая

Характеристики организационных структур ОУ ОС, представленных номерами уровня в таблице 3, следующие:

1 − по каналам связи информационный поток направленный, по каналам обратной связи - направленный, типы обучающих воздействий на обучающегося: представление обучающемуся информации, соответствующей специфике его деятельности, задача ОС;

2 − по каналам прямой и обратной связи информационные потоки рассеянные, типы обучающих воздействий аналогичны структуре 1;

3 − по каналам прямой связи информационный поток рассеянный, каналов обратной связи нет, тип обучающих воздействий: представление обучающемуся информации, соответствующей специфике его деятельности;

4 – каналов прямой связи нет, по каналам обратной связи информационный поток рассеянный, тип обучающего воздействия: задача ОС.

Исходными данными для метода определения оптимального уровня автоматизации и интеллектуализации функций управления ОС по подготовке специалистов по управлению объектами морской инфраструктуры являются решения, принятые на этапе определения состава стратегий ОС, а также сформулированные на общедидактическом уровне цели ОС, характеристика технологий реализации способов ОУ ОС и оценивания целесообразности автоматизации соответствующих функций ОУ ОС. Состав стратегий ОС может быть определен на основе положения педагогики об оптимизирующем и трансформирующем подходах к взаимосвязи этих стратегий, которые рассматривают два вида стратегий: базовые и вспомогательные. Выбор базовой стратегии ОС является важнейшей задачей, определяющей способы и технологии автоматизированного ОУ ОС с использованием средств автоматизации. Цели ОС определяются тем, какой из уровней формирования умений и навыков должен быть достигнут в результате реализации мероприятий ОС, что иллюстрирует таблица 4.

Таблица 4

Классификация уровней формирования умений и навыков

Номер уровня	Характеристика уровня
α_1	Узнавание объектов и явлений, присущих проводимому мероприятию ОС при повторном восприятии ранее усвоенной информации о них или действий с ними (деятельность на основе заданного алгоритма)
α_2	Репродуктивные действия, т.е. самостоятельное воспроизведение или применение информации о ранее усвоенной ООД (решение известных задач по известному алгоритму)
α_3	Продуктивные действия, т.е. самостоятельное построение или трансформация известной ООД по образцу из некоторого множества объектов, (решение типовых задач с использованием обобщенного алгоритма)
α_4	Творческие действия, т.е. самостоятельное конструирование новой ООД, выполняемое из множества известных объектов (продуктивная эвристическая деятельность, т.е. разработка алгоритма решения нетиповой задачи)

Выбор характеристик технологий реализации способов ОУ ОС от числа обучающихся представлены в таблице 5.

Таблица 5

Выбор характеристик технологий реализации способов ОУ ОС

Число обучающихся в ОС	Вид технологии реализации способа управления эффективностью ОС							
	С использованием КСА						Без использования КСА	
	A	B	C	D	E	F	G	H
$1<n<7$	$4, \alpha_4$		$3, \alpha_4$	$1, \alpha_4$	$2, \alpha_4$	—	$2, \alpha_4$	—
$n=7$	$4, \alpha_3$		$2, \alpha_3$	$3, \alpha_3$	$1, \alpha_3$	—	$1, \alpha_3$	—
$n>7$	—	—	—	—	—	$4, \alpha_1$-α_2	—	$4, \alpha_1$-α_2
$n>>7$	—	—	—	—	—	$4, \alpha_1$-α_2	—	$4, \alpha_1$-α_2

Примечание: 1) $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ – уровни формирования умений и навыков в ходе ОС, 2) *n* - число обучающихся, 3) *A* - автоматическое ОУ ОС, \z4) *B* – автоматизированное управление по варианту управления технологическим процессом, 5) *C* - автоматизированное управление по варианту нетехнологизированного управления обучающимися, 6) *D* - ручное управление с обработкой данных на ЭВМ, 7) *E* - ручное управление на основе ЭВМ, 8) *F* - неадаптивное программное управление на основе ЭВМ, 9) *G* - ручное управление, 10) *H* - ручное вырожденное управление. Ниже представлен алгоритм определения целесообразности автоматизации функций ОУ ОС:

1. Определение рангов (α_i) формирования умений и навыков для неавтоматизированной и автоматизированной технологий реализации способа ОУ ОС по результатам экспертного опроса.
2. Определение соотношения рангов ($\Delta\alpha$) сравниваемых технологий реализации способа ОУ ОС путем экспертного опроса.
3. Экспертное прогнозирование эффективности функций ОУ ОС путем установления предпочтения между неавтоматизированной и автоматизированной технологиями.
4. Экспертное прогнозирование эффективности функций ОУ ОС путем установления предпочтения между неавтоматизированной и автоматизированной технологиями.
5. Экспертное оценивание степени влияния на достижение целей ОС (по определенным мероприятиям, в целом) неавтоматизированной технологии реализации способа ОУ ОС.
6. Ранжировка экспертами автоматизированных и неавтоматизированных вариантов технологий реализации способов ОУ ОС по группам внедрения способов.
7. Экспертное оценивание целесообразности автоматизации функций ОУ ОС по группам внедрения способов (технологий) управления.

Заключение.

Установлено, что повышение эффективности ОУ ОС сопряжено с созданием и внедрением в процесс ОС будущих специалистов по управлению объектами морской инфраструктуры различного рода автоматизированных систем (АСУ, АС ППР, ЭС). Конкретно, необходимо использовать средства автоматизации в организационной и дидактической подсистемах ОУ ОС, которая в целом должна перейти в класс автоматизированных систем.

Достижение целей АС ОУ ОС должно базироваться на соблюдении двух групп принципов: организационных и технических. В состав организационных принципов входят принципы: системности, соответствия, целесообразности, психологичности и непрерывности. В техническую группу входят принципы: типизации и унификации, сбалансированности, гибкости, согласованности, модульности и приемлемости.

Определены виды автоматизированных систем, с которыми должна взаимодействовать АС ОУ ОС в рамках АСУ. Для решения задачи внедрения КСА в АС ОУ ОС разработаны принципы определения оптимального уровня автоматизации и интеллектуализации функций управления при подготовке специалистов по управлению объектами морской инфраструктуры. Они должны базироваться на соблюдении технологии психолого-педагогического проектирования и использовании наиболее эффективных способов ОУ ОС. Для этого выделены четыре группы внедрения способов ОУ ОС с использованием технологий, включающих КСА, и определена степень срочности их внедрения.

Определен перечень видов технологий реализации способов ОУ ОС с использованием КСА в зависимости от организационной структуры АС ОУ ОС, числа обучающихся и требуемого уровня формирования умений и навыков. Для решения названных задач разработана методика экспертного оценивания целесообразности автоматизации функций ОУ ОС.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев С.А., Гончар А.А., Стахно Р.Е. Моделирование структуры и процесса организационного управления тренажерной подготовкой в образовательных учреждениях правоохранительных органов. // Журнал «Вестник полиции» 5(1) - 2018 г., С. 3-9.
2. Алексеев С.А., Гончар А.А., Стахно Р.Е. Основы квалиметрии, автоматизации и интеллектуализации систем организационного управления практической подготовкой в вузах МВД. // Наука, техника и образование. № 5 (35) Москва. изд. «Проблемы науки». 2017. - С. 29-32.
3. Алексеев С.А., Стахно Р.Е. Вопросы организационного управления содержанием практической подготовки в вузах МВД. // Проблемы современной науки и образования № 19 (101). Москва. изд. «Проблемы науки». 2017. С. 19-22.
4. Губинский А.И., Евграфов В.Г. Эргономическое проектирование судовых систем управления. – Л.: Судостроение, 1977. – 224с.: ил

УДК 681.3

МОНИТОРИНГ ОБЪЕКТОВ МОРСКОГО И РЕЧНОГО ТРАНСПОРТА С ПОМОЩЬЮ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Балса Алдрин Раульевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mail: BalsaAR@gumrf.ru

Аннотация. Рассмотрена проблема мониторинга объектов морского и речного транспорта в двух аспектах: мониторинг состояния и мониторинг перемещения в пространстве.

Ключевые слова: мониторинг; управление; наблюдение; водный транспорт; информационные технологии.

OBJECTS' MONITORING OF THE MARITIME AND INLAND TRANSPORT BY MEANS OF MODERN INFORMATION TECHNOLOGIES

Balsa Aldrin
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya Str., St. Petersburg, 198035, Russia
e-mail: BalsaAR@gumrf.ru

Abstract. The problem of monitoring of objects of the maritime and inland transport in two aspects is considered: monitoring of their physic conditions and of their location.

Keywords: monitoring; control; observation; water transport; information technologies.

Введение.

С каждым годом информационные технологии становятся все более значимыми. Сегодня информационные технологии используются практически во всех сферах жизни общества. Это не только компьютерные системы, защита информации, бухгалтерский учет, системы принятия решений, но и такие задачи как оптимизация производства и торговли, оптимизация оказания государственных услуг гражданам, мониторинг и анализ эффективности оборудования, и многие другие.

В сфере перевозок грузов и пассажиров с использованием водного транспорта так же активно применяются информационные технологии. Внедрение информационных технологий делает процесс управления огромным количеством судов гораздо менее сложным.

В России доставка грузов и перевозка пассажиров с использованием водного транспорта занимают особое место [1]. Это обусловлено огромными водными просторами на территории нашей страны: около 146 тыс. км водных путей могут использоваться речным транспортом, а морской транспорт необходим для сообщения с другими материками. Есть и другой путь – по воздуху, но для его использования требуется слишком много ресурсов для создания средств передвижения и топлива для его использования. Кроме того, этот путь крайне ненадежен – нередки аварии, влекущие за собой человеческие жертвы, материальные потери и нанесение вреда экологии.

На Рис. 1. Судоходная сеть России. По ней прослеживается необходимость использования водного транспорта в стране: в некоторые регионы нет возможности осуществить доставку грузов, не используя судоходные пути из-за особенностей рельефа, погодных условий или других причин.

В пользу водного транспорта говорит и материальная составляющая: гораздо дешевле использовать уже существующие природные пути, чем строить их, загрязняя окружающую среду. Использование морского и речного транспорта оказывает наименьшее влияние на состояние окружающей среды при выполнении действий по минимизации этого влияния. Для этого необходимо регулярно проводить модернизацию оборудования, позволяющую вводить в оборот новые технологии, обеспечивающие большую надежность и меньший вред для окружающей среды.

Таким образом, водный транспорт является наиболее экологичным, дешёвым и быстрым способом доставки грузов и перевозки пассажиров. В процессе его использования возникают проблемы по обслуживанию объектов водного транспорта. Среди них выделяется проблема мониторинга [2, 3, 4, 5], которая имеет два аспекта:

- Мониторинг состояния объектов морского и речного транспорта;
- Мониторинг перемещения объектов морского и речного транспорта в пространстве.

Относительно мониторинг состояния объектов морского и речного транспорта необходимо вовремя проводить модернизацию, ремонт и списание судов для их эффективного использования. Для небольших компаний, которые не могут позволить себе иметь платную программу 1С:Предприятие, альтернативой может стать программа Microsoft Access, которая стоит гораздо дешевле. Эта программа предназначена для работы с базами данных с использованием языка запросов SQL. Для каждого порта целесообразно иметь отдельную таблицу, содержащую графы «Идентификационный номер судна», «Название судна», «Дата спуска на воду», «Состояние судна». Сопровождение такой таблицы легче осуществлять с помощью встроенных средств Microsoft Access, таких как запросы, формы, отчеты и т.д.

Рис. 1. Судоходная сеть России

С помощью языка запросов SQL можно легко выбрать нужные суда для корректирования информации о них, добавлять новые суда и удалять записи о списанных судах.

Так как существует огромное множество бесплатных аналогов этой программы для работы с базами данных, стоит вопрос об удобстве их использования. Для добавления или удаления большого количества судов в разные порты вручную – очень трудоемкая задача, требующая немало времени. Для оптимизации редактирования базы данных можно создать отдельное приложение, ориентированное на решение определенных задач для конкретной базы данных. В таком приложении выгодно сделать удобный интерфейс, не требующий знания языка запросов SQL. Недостаток такого решения в том, что для другой базы данных потребуется создание нового приложения. Гораздо удобнее, если база данных будет доступна не только с того компьютера, на котором установлено приложение, но и для других компьютерных систем. Для этого целесообразно создавать web-приложение, клиентская часть которого доступна через браузер.

Кроме мониторинга за состоянием судов необходимо контролировать их перемещения. Это важно не только для своевременного оповещения участников перевозки об изменениях и задержках, но и для уменьшения времени, необходимом для проведения профилактических и ремонтных работ. В зависимости от местности, в которой побывало судно, ему могут потребоваться дополнительные процедуры по устранению последствий плавания. Целесообразно заранее приготовить нужные материалы для устранения неполадок, чтобы судно не простаивали, следовательно, нужно как можно более точно определить время его прибытия в порт.

Другая ситуация: шторм отнес судно от намеченного пути. Для пополнения запасов провизии и топлива ему необходимо зайти в ближайший порт. Узнав об этом, можно заблаговременно выкупить место для стоянки и материалы для ремонта, сократив время задержки судна в пути.

Наиболее распространенным способом для определения местоположения объектов наблюдения является спутниковая система навигации [6]. В современном мире существует несколько таких систем, принадлежащие разным странам. Крупнейшими из них являются:

- ГЛОНАСС, РФ, 24 спутника;
- GPS, США, 31 спутник.

Существует огромное множество разнообразных средств, которые не только определяют местоположение объекта, но и собирают и систематизируют информацию о положении объекта в пространстве. Большинство из них используют спутниковая система навигации GPS.

Заключение.

Состояние и развитие транспорта имеют для Российской Федерации исключительное значение. Транспорт, наряду с другими инфраструктурными отраслями, обеспечивает базовые условия жизнедеятельности общества, являясь важным инструментом достижения социальных, экономических, внешнеполитических целей. Транспорт - не только отрасль, перемещающая грузы и людей, а, в первую очередь, межотраслевая система, преобразующая условия жизнедеятельности и хозяйствования. Таким образом, мониторинг состояния и перемещения объектов водного транспорта является важной задачей для государства, а современные технологические средства призваны помочь ее решить.

СПИСОК ЛИТЕРАТУРЫ

1. Транспортная стратегия Российской Федерации на период до 2030 года // Официальные сайты органов государственной власти Российской Федерации: Совет Безопасности Российской Федерации // [Электронный ресурс] – Режим доступа: http://www.scrf.gov.ru/security/economic/document123, свободный. – Загл. с экрана.
2. Ю.Г. Вишневский. Инфокоммуникационные технологии для обеспечения безопасности передачи сообщений мониторинга и управления в речных автоматизированных системах управления движением судов: автореферат дис. д-ра техн. СПб. : ФГОУ ВПО СПГУВК, 2008. 51 с.
3. А.А. Сикарев. Системы мониторинга и управления судами технического и вспомогательного флота на внутренних водных путях России: дис. д-ра техн. наук. СПб. : ФГБОУ ВПО «ГУМРФ им. адмирала С. О. Макарова», 2013. 308 с.
4. А. В. Вотинов, С. В. Даценко. Совершенствование информационной системы мониторинга состояния и возможности предупреждения техногенных чрезвычайных ситуаций на транспортных комплексах // Водные пути России: строительство, эксплуатация, управление: международная научно-практическая конференция, посвященная 200-летию подготовки кадров для водного транспорта России. СПб. : ФГОУ ВПО СПГУВК, 2010. С.48-51.
5. Д. А. Акмайкин, Д. Б. Хоменко, С. Ф. Клюева. Обзор функциональных возможностей и перспективы современных автоматизированных систем планирования маршрута судна // Вестник Государственного университет морского и речного флота имени адмирала С. О. Макарова. СПб. : Изд-во ГУМРФ им. адм. С. О. Макарова, 2017. Т.9. С . 237-251.
6. С. Ф. Шахнов, А. А. Агеева. Построение системы контроля дифференциальной подсистемы ГЛОНАСС/GPS с использованием метода математической обработки параметров сигнала дифференциальной поправки // Вестник Государственного университет морского и речного флота имени адмирала С. О. Макарова. СПб. : Изд-во ГУМРФ им. адм. С. О. Макарова, 2017. Т.9. С . 402-413.

УДК 658.58

АЛГОРИТМИЗАЦИЯ АВТОМАТИЧЕКОЙ СИСТЕМЫ ВИБРАЦИОННОЙ ДИАГНОСТИКИ СУДОВОГО РОТОРНОГО ОБОРУДОВАНИЯ

Баркова Наталия Александровна[1], Грищенко Дмитрий Вячеславович[2]
[1] Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
[2] Северо-Западный учебный центр
Стачек пр., 140, Санкт-Петербург, 198207, Россия
e-mails: barkova@vast.su, gri_dmi@mail.ru

Аннотация. Рассматривается решение ряда проблем алгоритмизации автоматической системы вибрационной диагностики судового роторного оборудования, а именно выделение диагностической информации и оценка изменения диагностических параметров во времени.

Ключевые слова: вибродиагностика; автоматизация; алгоритмы; стационарная система; пороги; анализ спектров; судовые роторные машины.

ALGORITHMS FOR AUTOMATIC DIAGNOSTIC SYSTEMS WICH USE VIBRATION SIGNALS

Barkova Nataliya [1], Grishchenko Dmitriy [2]
[1] St. Petersburg State Marine Technical University
3 Lotsmanskaya Str., St. Petersburg, 190121, Russia
[2] Severo-Zapadnyj uchebnyj centr
140 Stachek Av., Saint Petersburg, 198207, Russia
e-mails: barkova@vast.su, gri_dmi@mail.ru

Abstract. The solution of some problems associated with the creation of algorithms for an automatic diagnostic system of marine rotary machines using vibration signal is considered, namely, the definition of diagnostic information and the assessment of the change in diagnostic parameters over time.

Keywords: vibrodiagnosis; automation; algorithms; stationary system; threshold values; spectrum analysis; marine rotary machines.

Введение.

К судовому оборудованию, отвечающему за безопасность плавания, в первую очередь, относится роторное оборудование энергетических систем. Для оценки его текущей работоспособности и прогноза состояния эффективным методом является вибрационный (не относится к механизмам с узлами возвратно поступательного действия) [1]. Из-за необходимости оперативного принятия решения при управлении ответственным оборудованием вибрационный метод целесообразно реализовывать в виде стационарных автоматических систем диагностирования, в которых для уточнения диагноза могут также использоваться параметры прочих физических процессов. При разработке таких систем должны учитываться особенности эксплуатации судна, такие как качка, нестабильность параметров питающей сети, флуктуации температуры, нагрузки и других условий, которые приводят к нестабильности частоты вращения и вибрационной активности, что требует применения специально разработанных для таких условий алгоритмов обработки информации. Все применяемые алгоритмы можно разделить на три основные группы в зависимости от типа решаемых задач: первая - обработка сигнала с целью извлечения диагсноических параметров, вторая - оценка диагностической значимости изменения полученных параметров, третья - автоматизация диагноза. В статье рассматривается ряд основных проблем алгоритмизации при решении первых двух из указанных задач.

Наиболее важную диагностическую информацию о состоянии роторных машин извлекают из узкополосных спектров вибрации, выделяя из него составляющие разной физической природы [1]. Для этого используются соответствующие алгоритмы, базовый из которых осуществляет поиск и выделение гармонических составляющих (гармоник). Обозначенный алгоритм включает две задачи: выделение отсчетов, соответствующих именно гармоническим составляющим и на основании их значений определение параметров гармоник (как минимум – частоты и уровня). Первая задача может быть решена за счет построения так называемой линии фона путём удаления сильных выбросов с последующим сглаживанием полученных данных [2]. Линия фона может использоваться как для оценки характера распределения случайных компонент, так и для выделения отсчетов гармонических составляющих, признаком которых является как раз значимое превышение фона. После выделения отсчетов спектра, соответствующих гармонике, решается задача определения ее параметров. Поскольку форма распределения отсчетов спектра около гармоники зависит от ее относительного положения по оси частот между ближайшими отсчётами, можно взять большое число таких промежуточных положений и определить зависимость поправки на частоту и амплитуду от соотношения уровней двух максимальных отсчетов спектра. Данную зависимость можно представить аналитически с помощью аппроксимации. Способ, реализующий такой подход, использован в виброанализаторе 2515 фирмы «Брюль и Къер» [3] и в программе DREAM 4 фирмы Ассоциация BACT.

При обработке спектров реального оборудования указанным способом, измеренных при девиации частоты вращения, особенно характерной для судовых условий, были получены значительные погрешности. Наиболее критичной является ошибка определения частоты, поскольку она влияет на корректность последующего анализа с целью поиска гармонических рядов. Данные ошибки связаны в первую очередь с тем, что при девиации частоты гармоника расширяется (как бы размазывается по соседним спектральным линиям), что приводит к изменению поправки на частоту и амплитуду без необходимости. Для минимизации ошибок предложен альтернативный способ, базирующийся на использовании интерполяционного метода, при этом подобрана параболическая функция для отсчетов спектра возведенных в четвертую степень. Аппроксимация производится по трем максимальным отсчетам спектра вблизи гармоники. Данная функция достаточно точно повторяет форму АЧХ канала спектра (использовалось окно Ханна) и позволяет получить существенно лучший результат по сравнению с приведенным выше способом (рис. 1)

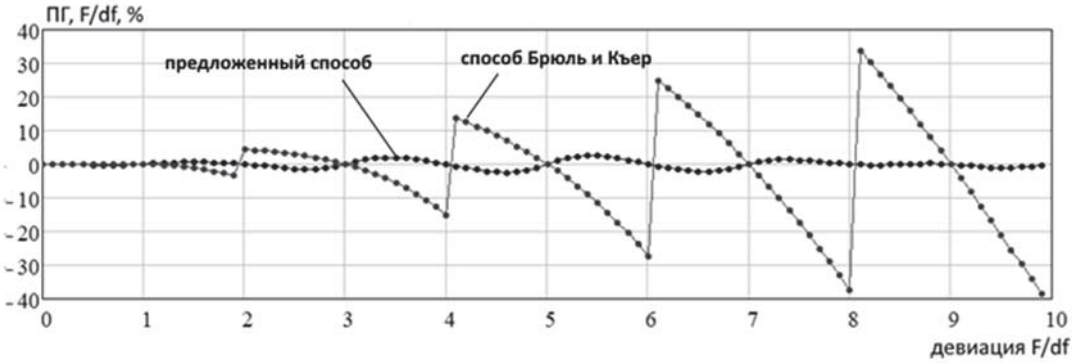


Рис. 1. Погрешность определения частоты вращения, полученная с помощью модельных сигналов с различной заданной девиацией частоты гармоники за время измерения спектра

Одной из основных особенностей работы оборудования в судовых условиях является влияние на виброактивность различных естественных факторов, к которым можно отнести качку, изменение температурного и прочих режимных параметров, таких как давление, расход (в случае потокопреобразующих агрегатов), нагрузка, частота питающей сети и пр. При этом изменения данных параметров различного рода отражаются и в изменениях вибрационных параметров. Стандарты предписывают в таком случае контролировать все влияющие факторы и на основании этого выделять различные режимы [4], для каждого из которых базовое значение, соответствующее бездефектному состоянию, определяется отдельно. Однако выделять режимы, учитывая все влияющие факторы проблематично и часто просто нецелесообразно, поскольку данные факторы могут быть несвязанными и многочисленными что приведет к необходимости выделения большого числа режимов (по числу возможных комбинаций) и в результате к большой путанице и неоднозначности. На практике, если параметр подвержен сильным монотонным флуктуациям, им или пренебрегают (не используют) или сильно заглубляют пороги отталкиваясь от уровня максимальных флуктуаций, обнаруженных за длительное время. Однако загрубение порогов приводит к запаздыванию обнаружения ухудшения состояния, из чего можно сделать вывод о необходимости поиска более эффективного метода, в качестве которого предложен метод адаптации порогов. Суть метода заключается в организации накопления данных на последовательных временных интервалах (накопителях) различной длительности, в каждом из которых производится оценка характерных флуктуаций и построение соответствующих пороговых значений. Так на рис. 2 показан график изменения уровня вибрации на частоте вращения турбины, входящей в состав промышленного турбогенератора. Из графика видно, что величина естественных флуктуации параметра на интервале в сутки (несколько суток) существенно меньше уровня флуктуаций за интервал сравнимый с месяцем, который определяет общий разброс. При этом обнаружение роста за сутки на величину значительно превышающую наблюдаемый ранее уровень разброса, соответствующий

данному временному интервалу, будет говорить об изменении состояния или о нетипичном режиме, хотя порог построенный стандартным способом на основании общего разброса не будет превышен еще долгое время.

Данные при передаче из одного накопителя в следующий сглаживаются и прореживаются, таким образом устраняются незначимые для конкретного временного интервала изменения и обеспечивается минимизация объема хранимой информации. Данный способ базируется на том, что влияние каждого конкретного фактора приводит к ограниченному изменению параметра в некотором интервале, который можно оценить, набрав определенную статистику. Как показывает опыт, наиболее высокий уровень монотонных флуктуаций характерен на временных интервалах большой длительности, что позволяет понизить пороги, установленные на интервалы меньшей длительности и быстрее реагировать на деградацию с высокой скоростью, что особенно актуально при обнаружении ошибок управления.

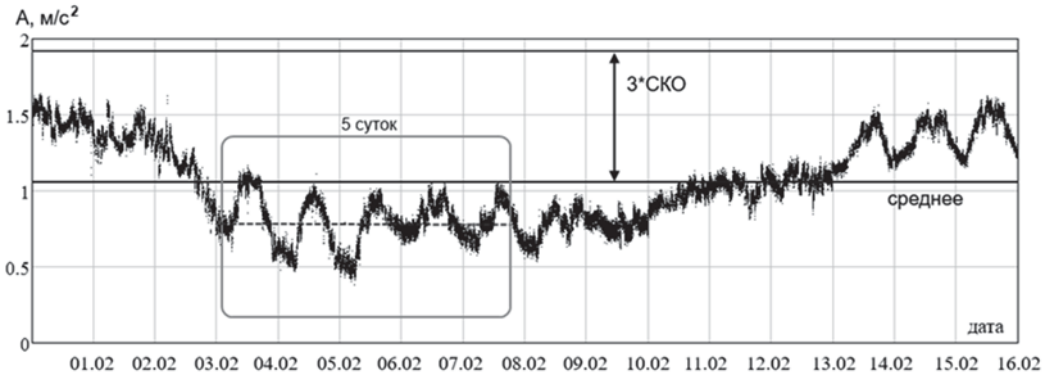


Рис. 2. Оценка разброса данных на временных интервалах различной длительности

Заключение.

Приведенные способы, решающие задачи обработки диагностической информации, опробованы на различных модельных сигналах и реальных сигналах роторного оборудования, в том числе судового, и доказали свою эффективность. Способы внедрены в виде программных моделей систем мониторинга и диагностики серии СМД4 производства ООО «Ассоциация ВАСТ», которые прошли заводские испытания и поставлены на различные объекты, в том числе для оснащения судового оборудования.

СПИСОК ЛИТЕРАТУРЫ

1. Неразрушающий контроль: Справочник в 7 т. Под общ. ред. В.В. Клюева, Т.7: В 2 кн. Кн. 2: Ф.Я. Балицкий, А.В. Барков, Н.А. Баркова и др. Вибродиагностика. – М.: Машиностроение, 2005. – 829 с.
2. Грищенко Д. В. Автоматическая обработка узкополосных спектров вибрации судовых машин в целях выделения диагностически значимых компонент // Морские интеллектуальные технологии. – 2016. – № 4 (34). Т. 2. – С. 8-13. – ISSN № 2073-7173
3. Рандалл Р. Б. Частотный анализ // Копенгаген: Брюль и Къер, 1989. – 389 с.
4. ГОСТ Р ИСО 13373-1-2009 Контроль состояния и диагностика машин. Вибрационный контроль состояния машин. Часть 1. Общие методы. – М.: Стандартинформ, 2010. – 43 с.
5. Грищенко Д. В. Система непрерывного мониторинга состояния и оперативной диагностики судового роторного оборудования // Вестник Астраханского государственного технического университета. Серия: Морская техника и технология. – 2016. – № 4. – С. 54-62. – ISSN 2073-1574.

УДК 658.58

ВОЗМОЖНОСТИ ВИБРАЦИОННОЙ ДИАГНОСТИКИ ГАЗОТУРБИННЫХ ДВИГАТЕЛЕЙ

Баркова Наталия Александровна[1], Грищенко Дмитрий Вячеславович[2]
[1] Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
[2] Северо-Западный учебный центр
Стачек пр., 140, Санкт-Петербург, 198207, Россия
e-mails: barkova@vast.su, gri_dmi@mail.ru

Аннотация. Рассматриваются вопросы вибрационной диагностики высокооборотных газотурбинных двигателей с учетом двух основных особенностей формирования и контроля их вибрации – высокого уровня случайной вибрации, возбуждаемой воздушным и газовым потоками и недоступностью большинства узлов для контактного измерения их вибрации, ограничивающих эффективность диагностирования механических узлов двигателя по формируемым в них колебательным силам. Предложены основное направление решения возникающих проблем, заключающееся в переходе на контроль вибрации в удаленных точках крепления двигателя к внешним конструкциям, и способы выделения и анализа составляющих вибрации, возбуждаемых вращающимися элементами силовых и вспомогательных узлов двигателя.

Ключевые слова: вибродиагностика; газотурбинные двигатели; узлы вращения; контроль вибрации; спектральный анализ; периодическая и случайная вибрация; диагностика на стабильной и нестабильной скоростях вращения.

THE CAPABILITYES OF GAS-TURBINE DIAGNOSTICS BY VIBRATION SIGNAL

Barkova Nataliya [1], Grishchenko Dmitriy [2]
[1] St. Petersburg State Marine Technical University
3 Lotsmanskaya Str., St. Petersburg, 190121, Russia
[2] Severo-Zapadnyj uchebnyj centr
140 Stachek Av., Saint Petersburg, 198207, Russia
e-mails: barkova@vast.su, gri_dmi@mail.ru

Abstract. The problems of vibration diagnostics of high – speed gas-turbine engines are considered taking into account two main peculiarities of vibration excitement and its control. These are - high level of random vibration excited by air and gas flows and the inaccessibility of most machine units for contact measurements of its vibration. It limits the effectiveness of engine mechanical components diagnosing by the oscillating forces excited there. The main direction of solving the arising problems is offered. It consists of vibration control in remote points of fastening the engine to external constructions, and ways of allocation and analysis of the vibration components excited by rotating elements of power and auxiliary units of the engine.

Keywords: vibration diagnostics; gas turbine engines; rotation units; vibration control; spectral analysis; periodic and random vibration; diagnostics at stable and unstable rotation speeds.

Компактные энергетические установки для транспорта все чаще строятся на основе высокооборотных газотурбинных двигателей, которые, как правило, определяют и надежность установки, и ее ресурс, поэтому вопросы контроля и прогноза технического состояния газотурбинных двигателей выходят на первый план. Вибрационная диагностика - одно из важнейших направлений и контроля, и прогноза технического состояния машин роторного типа, но применительно к газотурбинным двигателям ее развитие сдерживается высоким уровнем вибрации, создаваемой потоками воздуха и продуктов сгорания, «маскирующей» вибрацию других узлов, определяющих надежность и ресурс двигателя. Кроме этого, в состав газотурбинного двигателя входят не только крупные узлы-источники основной вибрации, такие как роторы компрессоров и силовых турбин, но и менее мощные узлы для пуска, смазки, отъема энергии на вспомогательные нужды и другие. Их вибрационная диагностика усложняется из-за еще меньшего уровня создаваемой вибрации и отсутствия влияния на формируемые потоки воздуха и газа. Наконец, выпускаемая в едином конструктивном блоке энергетическая установка может включать в себя и редуктор, и другой вид машин, например, электрогенератор, что существенно усложняет спектральный состав контролируемой вибрации.

В настоящее время вибрационный контроль текущего состояния газотурбинных двигателей, как правило, выполняется по широкополосному (третьоктавному), а для силовых валов, и по узкополосному спектру вибрации в специально подобранных контрольных точках. Он обеспечивает обнаружение опасных изменений состояния валов и рабочих колес компрессора и силовой турбины, но не дает возможности выявлять дефекты других узлов, в том числе подшипников, вплоть до возникновения предаварийного состояния, т.е. используется для аварийной защиты. Для более ранней диагностики газотурбинного двигателя необходимо существенно увеличивать частотное разрешение в контролируемых спектрах вибрации, оптимизировать точки контроля вибрации и диагностировать энергетическую установку в целом. Такой подход к вибрационной диагностике газотурбинных двигателей реализуется, прежде всего, при высокой стабильности скорости вращения всех валов газотурбинной установки.

Первая из внедренных нами стационарных систем вибрационной диагностики для газотурбинного двигателя в составе электрогенерирующей установки имела общий для компрессора и силовой турбины вал (двигатель Taurus-70, частота вращения 15000 об/мин). В этой установке стабильность частоты вращения обеспечивалась жесткой связью валов двигателя, редуктора и электрогенератора, подключенного к сети предприятия «ОАО Балтика», а относительная «простота» спектра вибрации – использованием в установке подшипников скольжения. Разрешение по частоте в измеряемых спектрах вибрации составило 1 Гц.

Несмотря на сложный спектральный состав вибрации установки (см. рис.1), измеряемой в нескольких точках на неподвижных частях двигателя, планетарного редуктора и синхронного четырехполюсного электрогенератора, система обеспечила выделение основных диагностических признаков типовых дефектов собственно двигателя, редуктора, генератора и общей системы смазки.

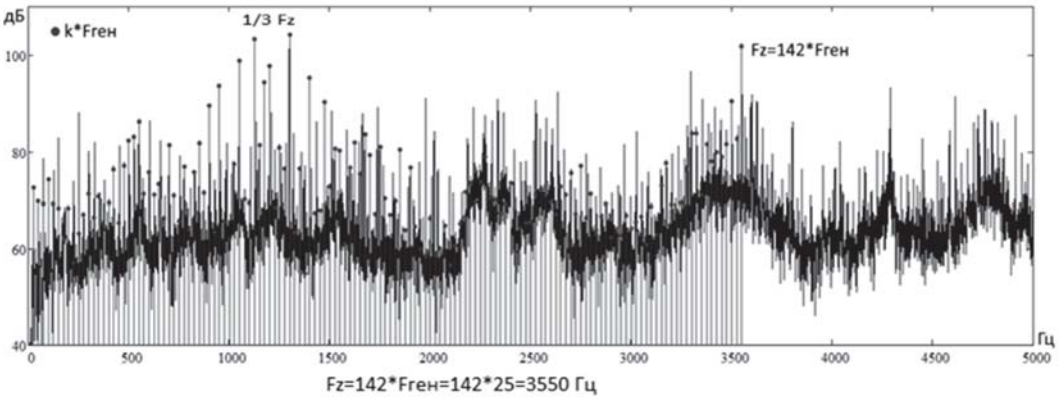


Рис.1. Спектр вибрации редуктора установки с признаками износа зубцов короны (рост вибрации на высоких, близких к 1/3 зубцовой частоты, гармониках частоты ее вращения), измеренный за месяц до срабатывания штатных средств аварийной защиты

Состояние короны на момент срабатывания средств защиты приведено на рис.2.

Рис. 2. Внешний вид короны редуктора установки, зафиксированный при ее дефектации

Три года эксплуатации системы диагностики показали возможность обнаружения и идентификации дефектов в узлах установки задолго (месяц) до возникновения реальной опасности для продолжения ее эксплуатации. Всего было выявлено три дефекта, потребовавших вмешательства ремонтных служб.

Параллельно на газоперекачивающих станциях ОАО «Газпром» выполнялись исследования вибрации агрегатов с авиационными газотурбинными двигателями, в рамках которых проводилась оценка возможности диагностирования подшипников качения классическими методами анализа подшипниковой вибрации. Эти исследования показали, что традиционными методами можно диагностировать только радиально-упорные подшипники, имеющие стабильную осевую нагрузку, а в других подшипниках на высоких скоростях вращения в подшипниковой вибрации могут происходить фазовые «скачки», искажающие ее спектры, и необходимо корректировать используемые методы вибрационной диагностики подшипников.

Кроме этого анализ вибрации многовальных газотурбинных двигателей, работающих в наземных условиях, показал, что при работе валов компрессора в установившихся режимах стабильность их частот вращения, обеспечиваемая средствами автоматического регулирования, недостаточна для диагностического анализа спектров вибрации, позволяющего выявить дефекты рабочих колес, подшипников качения и зубчатых зацеплений валов. Так, как показано на рис.3, практически достижимая стабильность частоты вращения валов составляет около 0,2%, а для анализа спектра на лопаточных частотах должна составлять не хуже 0,02%.

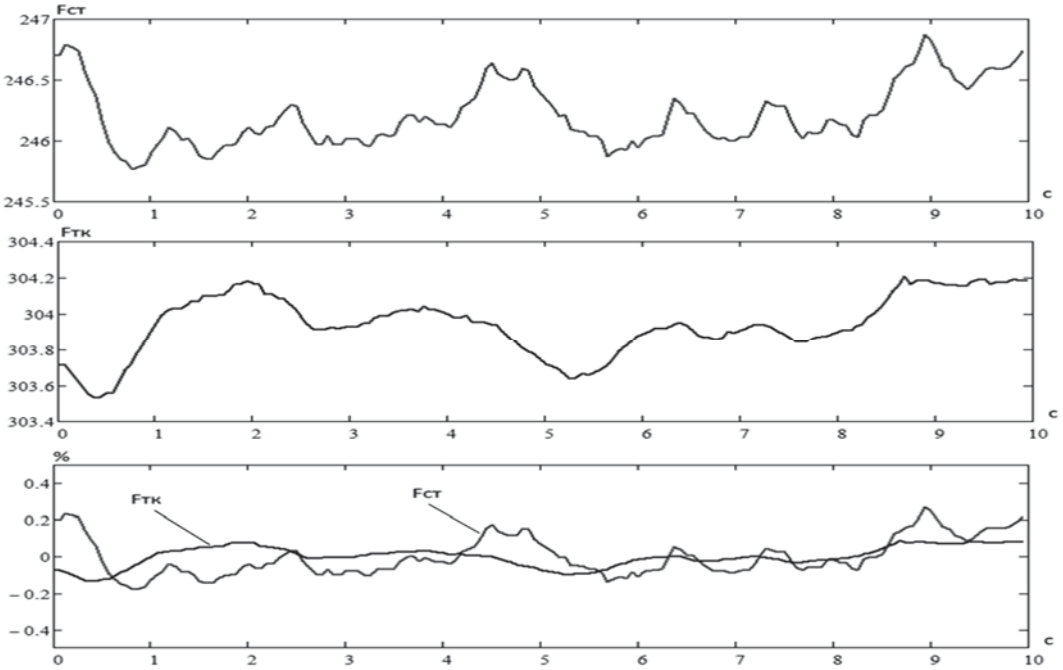


Рис.3. Зависимость частоты вращения компрессора - a) и частоты вращения силовой турбины - b) от времени газотурбинного двигателя в автоматическом режиме его работы. На нижнем графике – c) совмещены обе зависимости, нормированные на их средние значения

Существующая нестабильность частоты вращения ограничивает частотное разрешение на лопаточных частотах на уровне 8 - 10Гц, чего не хватает для выделения многих гармоник на фоне случайной вибрации, возбуждаемой потоками воздуха и продуктов горения, см. рис.4.

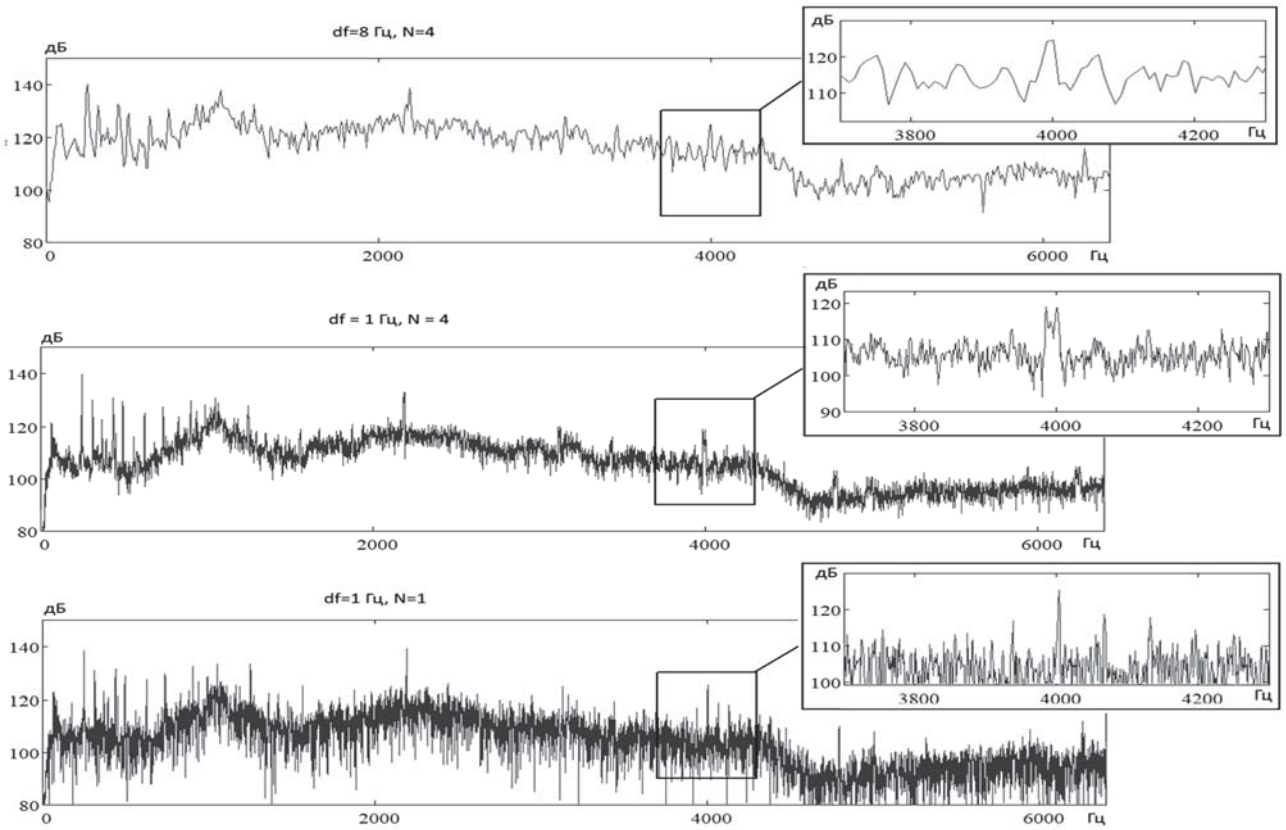


Рис.4. Спектры вибрации авиационного газотурбинного двигателя в точке его крепления к несущим конструкциям, измеренные с разным разрешением df и разным количеством усредняемых спектров N

Как следует из анализа приведенных спектров, достаточное для диагностики зубчатых зацеплений и рабочих колес разрешение по частоте составляет 1Гц, но усреднение нескольких спектров, необходимое для снижения статистического разброса случайных составляющих, приводит к «размыванию» гармонических составляющих спектра. Решать эту проблему можно тремя путями – повышать точность стабилизации частот вращения силовой турбины и компрессора, переходить на измерение порядковых спектров или разрабатывать методы повышения точности обработки спектров без их усреднения. Поскольку точность стабилизации частоты вращения на существующих двигателях повысить невозможно, как и измерять порядковые спектры вибрации при неплавных и разнонаправленных изменениях частот вращения валов одного агрегата, в данной работе использованы нетрадиционные методы обработки спектров вибрации, измеряемых без усреднения и в те короткие интервалы времени в 1-2с., когда оба независимо регулируемых вала компрессора и силовой турбины имеют практически стабильные частоты вращения.

Существует и еще один практический путь диагностирования газотурбинных двигателей – при принудительном вращении его валов от внешнего привода на пониженных частотах вращения, когда резко снижаются уровни случайных составляющих вибрации от воздушного потока и можно на время измерений обеспечить высокую стабильность скорости его вращения. Диагностику двигателя можно в этом случае выполнять между плаваниями (полетами).

Так на рис.5 приведены спектры вибрации одинаковых двигателей, измеренных в одной и той же точке контроля в номинальном режиме работы и на стенде, при скорости вращения в 10 раз ниже.

Анализ спектров показывает, что уровень случайной вибрации, возбуждаемой потоком, при принудительном вращении ротора снижается в низкочастотной части спектра более, чем в 100 раз, в то время как уровень многих гармонических составляющих, отвечающих за разные дефекты – менее, чем в 10 раз. Это открывает расширенные возможности обнаружения дефектов подшипников качения и зубчатых зацеплений на более ранней стадии развития по вибрации, измеряемой в местах крепления двигателя к несущим конструкциям.

Все необходимые алгоритмы диагностики многовальных газотурбинных двигателей разработаны и внедряются в новую версию стационарной и стендовой систем вибрационной диагностики агрегатов с газотурбинными двигателями.

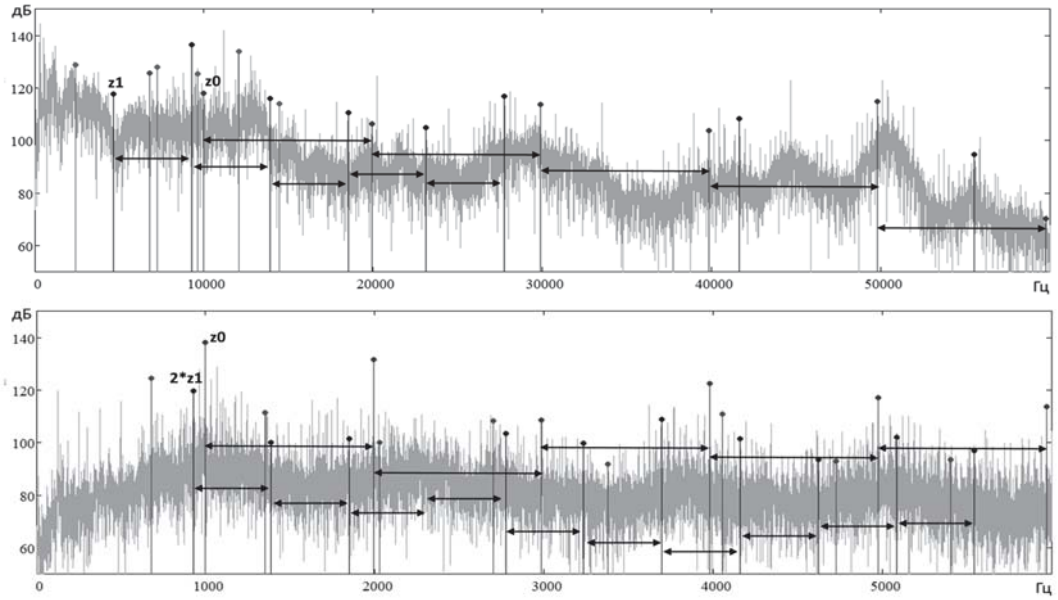


Рис.5. Спектры вибрации газотурбинного двигателя в номинальном режиме работы, измеренные в частотном диапазоне до 60кГц (верхний спектр) и при принудительном вращении с частотой в 10 раз ниже, измеренные в частотном диапазоне до 6кГц (нижний спектр)

Выводы.

1. Для контроля состояния газотурбинных двигателей в номинальных режимах работы применимы не все типовые методы вибрационного диагностирования роторных машин, во-первых, из-за высокого уровня вибрации, возбуждаемой газовыми потоками, а, во-вторых, из-за сложности установки датчиков на неподвижные части узлов вращения двигателя.

2. Эффективным является вибрационное диагностирование газотурбинных двигателей по узкополосному спектру вибрации, измеряемой в удаленных точках контроля, но при частотном разрешении не хуже 1 Гц, повышающем отношение сигнал/шум до достаточных для ранней диагностики значений.

3. Для диагностирования лопаточного аппарата и зубчатых передач двигателя по гармоническим составляющим вибрации с частотами выше 2-4 кГц необходимо во время измерений обеспечивать стабильность частоты вращения всех турбин значительно выше 0,1 %, что не всегда возможно при его работе в естественных условиях.

4. Операции диагностирования газотурбинных двигателей можно проводить периодически между выходами в море (полетами) при вращении валов компрессора и силовой турбины от внешнего привода на низких оборотах, что позволит обеспечить либо стабильную частоту вращения, либо переход на использование порядковых спектров вибрации, а также существенно снизить шумы потоков и, тем самым, расширить номенклатуру используемых методов диагностики двигателя.

СПИСОК ЛИТЕРАТУРЫ

1. Неразрушающий контроль: Справочник в 7 т. Под общ. ред. В.В. Клюева, Т.7: В 2 кн. Кн. 2: Ф.Я. Балицкий, А.В. Барков, Н.А. Баркова и др. Вибродиагностика. – М.: Машиностроение, 2005. – 829 с.
2. Баркова Н.А., Грищенко Д.В. Возможности эксплуатационной диагностики планетарных редукторов на морском транспорте // Региональная информатика и информационная безопасность. Сборник трудов. Изд: СПОИСУ. СПб, 2016. С. 406-411.
3. Киселев Ю.В., Епишев Н.И. Диагностирование газотурбинных двигателей и их узлов по термогазодинамическим и виброакустическим параметрам: Учебное пособие // Самара: СТАУ, 2017, 189 с.

УДК 004.6

КВАЛИМЕТРИЧЕСКОЕ РАНЖИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА CRM, А ТАКЖЕ ЛУЧШИХ ПРАКТИК ИХ ОСВОЕНИЯ В ЖИЗНЕННОМ ЦИКЛЕ ОБЪЕКТА МОРСКОЙ ТЕХНИКИ ТИПА СУДОВАЯ РАДИОЛОКАЦИОННАЯ СТАНЦИЯ

Бекетова Екатерина Александровна
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mail: kat-bek@mail.ru

Аннотация. Выполнен анализ использования информационных технологий класса CRM в интересах обоснования и оптимизации выбора конкурентноспособного варианта их реализации. Определены конкурентные преимущества применения программного комплекса класса CRM применительно к объекту морской техники типа судовая радиолокационная станция.

Ключевые слова: радиолокационная станция; система; CRM-технологии; bpm’online.

KVALIMETRIC RANGE OF INFORMATION TECHNOLOGIES OF THE CLASS CRM, AND THE BEST PRACTICES OF THEIR DEVELOPMENT IN THE LIFE CYCLE OBJECTS OF MARINE TECHNOLOGY TYPE SHIP RADAR STATION

Beketova Ekaterina
St. Petersburg State Marine Technical University
3 Lotsmanskaya Str., St. Petersburg, 190121, Russia
e-mail: kat-bek@mail.ru

Abstract. An example of using information technologies of the CRM class is given, and their work is described. The advantages of using programs are determined.

Keywords: radar; system; CRM technology; bpm'online.

При обосновании развития объектов морской техники (ОМТ), в том числе типа судовая радиолокационная станция, весьма актуальным является решение сложной проектной задачи квалиметрического ранжирования и выбора для производственного использования информационных технологий (ИТ) класса CRM, а также лучших практик их освоения в жизненном цикле ОМТ.

Customer Relationship Management (CRM) - прикладное программное обеспечение для производственных организаций, предназначенное для автоматизации стратегий взаимодействия с заказчиками. «Стратегическая модель» ИТ данного класса основана на использовании управленческих и ИТ, с помощью которых компания собирает информацию о своих клиентах на всех стадиях его жизненного цикла, начиная с проектирования и производства до снятия с эксплуатации.

При этом в качестве заказа могут рассматриваться различные сложные ОМТ (корабли, автомобили, самолёты и ракеты, компьютерные сети и др.), среди которых ниже рассмотрены радиолокационные станции (РЛС).

Результатом применения данного комплекса организационно-технических решений является повышение конкурентоспособности компании (КС) и увеличение прибыли, так как правильно построенные отношения, в том числе основанные на персональном подходе к каждому клиенту, позволяют привлекать новых клиентов и помогают удержать «старых».

Благодаря применению автоматизированной централизованной обработки данных появляется возможность эффективно и с минимальным участием сотрудников учитывать индивидуальные потребности заказчиков, а за счёт оперативности обработки — осуществлять раннее выявление рисков и потенциальных возможностей [1].

Требования, предъявляемые к CRM-системам при формировании и реализации заказов, могут быть сформулированы следующим образом:

– Актуальность, надежность и ценность (например, по критерию А.А. Харкевича) используемой информации, в том числе полученной в результате обработки данных.

– Результаты анализа продаж и качества их визуализации. Например, чтобы, глядя на один экран, заказчик имел представление о динамике работы отдела, направления развития, тренды и т.п.

– Сегментация и структуризация данных, включая данные по автоматизации процесса взаимодействия с заказчиками.

– Комплексная визуализация наиболее значимой информации, позволяющая оперативно, не более, чем в «3 клика», производить эффективный поиск дополнительных данных.

Согласно данным базы проектов TAdviser [3], на мировом рынке CRM-систем по количеству внедрений лидируют решения: «bpm'online» занимает первую строчку в рейтинге (по состоянию на октябрь 2017 года).

CRM-технология имеет следующие системные возможности (на примере bpm'online):

– эффективное управление производственной деятельностью организации;
– омниканальность;
– анализ больших данных;
– персонификация программ лояльности;
– использование технологий искусственного интеллекта;
– использование возможностей мобильных и облачных технологий;
– удобство интерфейса и другие.

Использование подобных систем дает предприятиям возможность производить продукцию высокого качества и обеспечивает заказчикам и пользователям наилучшие преимущества в работе с конкретными видами продуктов.

Еще более значимой является интеграция технологий CRM с ИТ других классов, что дает новые возможности и открывает такие сферы, где потенциал связанного с изделием интеллектуального капитала реализуется внутри расширенного предприятия.

В процессе апробации нами программы bpm'online были выявлены следующие свойства и её особенности:

– разработчики предлагают клиентам собственное видение бизнес□процесса;
– продажа настраивается под определенные потребности клиента;
– по результатам выполненного SWOT – анализа выявлены сильные и слабые стороны компании в сравнении с аналогичными по продуктам предложениями конкурентов;

– возможность работать с данными bpm'online CRM в режиме off-line, обеспеченная наличием специального расширения bpm'online Outlook Connector;

– возможность создания гибких адаптивных информационных систем в зависимости от изменений бизнес-процесса;

– удобство автоматического поиска контактов (номеров телефона), профиля в социяльных сетях, email-адресов и другие [4].

В наше время радиолокационная станция перестала быть редкостью на борту даже маломерных судов. Именно РЛС позволяет современному судоводителю уверенно чувствовать себя в самых сложных навигационных условиях, как в рубке океанского лайнера, так и на прогулочной яхте. Современная бортовая РЛС позволяет с высокой точностью и информационно комфортно отображать окружающую обстановку.

Основные условия, в которых используются радиолокационные станции, это - темное время суток, плохая видимость, туман, дождь, шторм и т.д. Соответственно, анализ свойств и характеристик современных CRM применительно к проектированию и эксплуатации судовых радиолокационных станций представляет практический интерес в плане безопасности плавания судов, обнаружения любого надводного объекта, а также навигационных опасностей в любых погодных условиях для гарантированного исключения аварийности судов.

В области производства и эксплуатации РЛС сложность продукции, её стоимость, расходы на содержание на стадии эксплуатации боевых кораблей возрастают во много раз по сравнению с гражданскими судами. Здесь следует учитывать две группы факторов – снижение затрат, в котором заинтересован как производитель продукции, так и заказчик.

К жизненному циклу заказа РЛС предъявляются жесткие требования:

– сокращение сроков проектирования и производства;

– повышения качества;

– снижение стоимости изделия и его эксплуатации на протяжении жизненного цикла;

– обеспечение высокой надежности и т.д.

Существует ряд проблем, которые возникают перед производителем РЛС [5]:

– ограничения по времени, как правило, при заключении контракта на поставку сроки поставки изделия заказчику, что являются одним из важнейших критериев выбора производителя;

– проблема качества. Необходимо обеспечить надлежащее качество при проектировании, производстве и техническом обслуживании. В понятие качество традиционно включается соответствие изделия техническому заданию и спецификации, т.е. обеспечение заданных технических и эксплуатационных свойств. Причем, стоимость исправления ошибок и брака при переходе на следующую ступень этого цикла возрастает в среднем на два порядка.

– проблема, вытекающая из предыдущих – потребность в снижении затрат, прямых и косвенных на проектирование и производство продукции.

– проблема взаимодействия различных организаций во время процесса производства продукции: организация - заказчик, конструкторское бюро, завод – строитель, смежники и т.д.

Результатом применения технологии CRM является повышение, как правило, конкурентоспособности и увеличение прибыли судостроительным компаниям, так как правильно построенные отношения, основанные на персональном подходе к каждому клиенту, позволяют привлекать новых клиентов и повышать лояльность имеющихся.

Представленная CRM-система «bpm'online» позволяет автоматизировать и сделать более продуктивными все процессы, присущие при заказе РЛС.

Выводы.

Благодаря CRM «bpm'online» практика эффективного бизнеса становится реальностью практически для любой компании.

Эффективное использование CRM - систем обеспечивает пользователям закрепление своих позиций на рынке, получение высокой прибыли и гарантированной рентабельности, а также обеспечение перспективы роста и развития.

В ближайшем будущем, по прогнозам экспертов, неизбежно развитие и совершенствование CRM-систем в части:

– исчезновения границ между CRM и другими системами;

– интеграции CRM в системы CEM, SaaS;

– появление интеллектуальных инструментов;

– развитие технологий омниканальных взаимодействий и поведенческого анализа;

– создание когнитивных сервисов, сервиса рыночных прогнозов и других.

СПИСОК ЛИТЕРАТУРЫ

1. [Электронный ресурс] – Режим доступа: http://bitconsulting.com.ua/crm/crm/o-sisteme-crm свободный. – Загл. с экрана. (Дата обращения 26.11.2018)
2. [Электронный ресурс] – Режим доступа: https://bit-24.ru/blog/rabota-s-bitriks24/that-should-be-able-crm-system-requirements-for-the-functionality/ свободный. – Загл. с экрана. (Дата обращения 24.11.2018)
3. [Электронный ресурс] – Режим доступа: http://www.tadviser.ru/index.php/ свободный. – Загл. с экрана. (Дата обращения 16.11.2018)
4. [Электронный ресурс] – Режим доступа: https://www.bpmonline.com/ свободный. – Загл. с экрана. (Дата обращения 14.11.2018)
5. ГОСТ Р 56135-2014 Управление жизненным циклом продукции военного назначения. Общие положения.

УДК 621.313.1

АВТОМАТИЗИРОВАННАЯ ОПТИМИЗАЦИЯ КОМПЛЕКТАЦИИ ГЕНЕРАТОРНЫМИ АГРЕГАТАМИ ЭЛЕКТРОСТАНЦИИ СПГ-ТАНКЕРА

Голубев Роман Олегович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mail: swit.roma@mail.ru

Аннотация. Статья посвящена исследованию вопроса автоматизированной оптимизации комплектации генераторными агрегатами вспомогательной судовой электростанции. Оптимизационная задача решается применительно к судам-транспортировщикам сжиженного природного газа с главными малооборотными двигателями. Цель оптимизации – повышение энергетической эффективности проектов и сокращение числа одновременно работающих генераторов. Задача решалась с применением программного комплекса расчётов и инженерного анализа (класса CAE). Рассмотрены следующие альтернативные варианты оснащения электростанции: двухтопливными агрегатами; двухтопливными агрегатами и утилизационными турбогенераторами; утилизационными турбогенераторами и валогенераторами. Определены области оптимального применения этих комбинаций.

Ключевые слова: валогенератор; сжиженный природный газ; система глубокой утилизации теплоты; судовая электростанция; судовая энергетическая установка.

SURVEY OF AUXILIARY GEN SET TYPES COMBINATIONS AUTOMATED OPTIMIZATION FOR LNG CARRIERS

Golubev Roman
St. Petersburg State Marine Technical University
3 Lotsmanskaya Str., St. Petersburg, 190121, Russia
e-mail: swit.roma@mail.ru

Abstract: The problem of optimal auxiliary gen sets combination choice for liquefied natural gas carriers equipped with low-speed main engines was explored by means of automated design system. The aims of optimization are projects` energy efficiency improvement and cutting number of generator sets in parallel. CAE information technology was applied to achieve these aims. Following schemes of auxiliary electrical power plant were examined: auxiliary power plant equipped with dual fuel gen sets only; dual fuel gen sets in parallel with turbines of waste heat recovery system; turbines of waste heat recovery system in parallel with shaft generators. Fields of this combinations optimal application were defined.

Keywords: shaft generator; liquefied natural gas; waste heat recovery system; auxiliary electrical plant; ship power plant.

Сегодня крупные СПГ-танкеры рефрижераторного типа, перевозящие сжиженный природный газ (СПГ) при атмосферном давлении и температуре –162°С, чаще всего оснащаются двигателями внутреннего сгорания. Их энергетические установки по типу судовой электростанции (СЭС) делятся на две группы: оснащённые единой электроэнергетической системой; с главными малооборотными двигателями (МОД) и вспомогательной СЭС.

В первом случае СЭС является главной, т.е. генерирует электроэнергию, необходимую для привода гребных винтов. Она же обеспечивает электроэнергией вспомогательную энергетическую установку и общесудовых потребителей. Электрогенераторы приводятся главными двухтопливными средне- или высокооборотными двигателями. Простота и однородность элементной базы СЭС значительно упрощает задачу выбора генераторных агрегатов.

Во втором случае сама СЭС относится к вспомогательной энергетической установке и её режим работы не связан жёстко с ходом судна. В наиболее простом случае она укомплектовывается дизель-генераторными агрегатами. Однако, во-первых, на СПГ-танкерах вместо дизель-генераторов могут применяться генераторы, приводимые двухтопливными двигателями, т.к. существует необходимость утилизировать испаряющийся в грузовых танках природный газ. Во-вторых, главные МОД имеют большую агрегатную мощность, создающую значительный ресурс утилизации, применимый для работы утилизационных паро- и газотурбогенераторов, а также комбинированных агрегатов. В-третьих, двигатели вспомогательной СЭС менее экономичны, чем главные МОД и имеют втрое меньший ресурс, поэтому встаёт вопрос о возможности привода генераторов напрямую от последних, реализуемой посредством валогенераторов (ВГ).

Так же в эксплуатации находятся СПГ-танкеры с паротурбинными энергетическими установками, но их доля в составе флота с каждым годом сокращается. Отсутствует перспективность развития этого типа установок ввиду их существенно меньшей экономичности и недостатка на бирже труда в необходимом количестве квалифицированных кадров, способных обеспечивать их эффективную эксплуатацию.

Оснащение СПГ-танкеров малооборотными двухтопливными двигателями внутреннего сгорания является наиболее перспективным. Однако, для энергетических установок с МОД существует множество возможных комбинаций типов генераторных агрегатов в составе СЭС. Далее рассмотрена методика оптимизации состава

СЭС различных классов СПГ-танкеров с МОД и результаты её применения к различным схемам комплектации электростанций.

1. Применение системы автоматизированного проектирования судовой энергетической установки для решения оптимизационной задачи. Существенно повысить достоверность и качество решения оптимизационных инженерных задач позволяют системы автоматизированного проектирования, реализующие информационные технологии класса CAE (англ. computer-aided engineering – системы расчётов и инженерного анализа).

Результаты, представляемые в статье, были получены с использованием программного комплекса (ПК) «LNGC-PP». Алгоритм оптимизации комплектации СЭС генераторными агрегатами, с применением системы автоматизированного проектирования, приведена на рис.1.

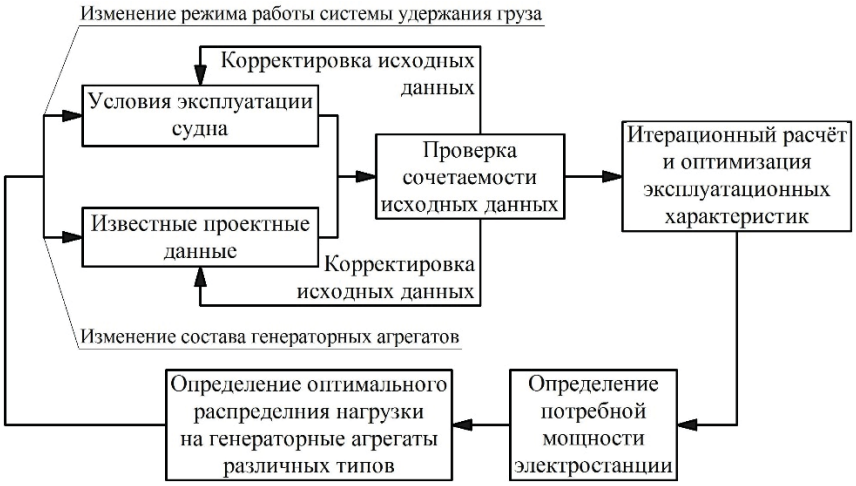


Рис. 1. Алгоритм автоматизированной оптимизации состава СЭС СПГ-танкера

Из приведённой схемы видно, что базой для проектирования электростанции является автоматизированный расчёт эксплуатационных характеристик проекта – условий работы пропульсивного комплекса и режима работы системы удержания груза. Далее программой определяется электрическая мощность, требуемая от электростанции для работы всего энергетического комплекса. После чего автоматически определяется оптимальное распределения нагрузки между электрогенераторными агрегатами различных типов, входящими в состав СЭС, и характеристики, однозначно определяющие режим их работы. Сами типы генераторных агрегатов, которые планируется применять на проекте, устанавливаются проектировщиком в исходных данных.

Результаты расчётов именно для этого этапа – определения типов генераторных агрегатов, удовлетворяющих наилучшим образом требованиям к СПГ-танкерам конкретного класса и проекта – изложены ниже. С особенностями работы самого автоматизированного ПК можно ознакомиться в [1].

2. Оптимальный тип топливопотребляющих генераторных агрегатов. Несмотря на существующее многообразие типов генераторных агрегатов, именно автономные генераторы (не зависящие от режима работы МОД) остаются основными в составе судовой энергетической установки (СЭУ). На ходу судна они либо полностью покрывают существующую потребность в электроэнергии, либо компенсируют недостающее количество электроэнергии, генерируемой агрегатами других типов. К тому же, без них невозможно обеспечение судна электроэнергией на стоянках и практически невозможна стабильная работа СЭС на переходных режимах пропульсивной установки.

Как было отмечено ранее, эти агрегаты могут быть как дизельными, так и двухтопливными. Двухтопливные рационально применять в тех случаях, когда главные МОД потребляют значительно меньше газа, чем испаряется в грузовых танках. Это условие устанавливается формулой (1).

$$\frac{S}{v_1}\left(\frac{BOR \cdot W}{24} - \frac{g_e^{ПГ\,ГД} \cdot N_{ГД}}{\rho_M}\right) \geq \frac{g_e^{ПГ\,ВД} \cdot N_{ВД} \cdot S}{\rho_M \cdot v_1}, \quad (1)$$

где BOR – суточная доля испарений груза; W – геометрический объём грузовых танков; $g_e^{ПГ\,ГД}$ и $g_e^{ПГ\,ВД}$ – соответственно удельный расход ПГ главных МОД и приводных двигателей вспомогательной СЭС; $N_{ГД}$ и $N_{ВД}$ – их эксплуатационные мощности; ρ_M – плотность метана (главного компонента СПГ); S – плечо рейса (расстояние, проходимое судном между терминалам экспортёра и импортёра); v_1 – скорость хода судна в грузу.

Это условие было проверено для СПГ-танкеров с грузовместимостью (W) от 140 до 300 тыс. м^3. Нижняя граница определяется практической невозможностью использования данного типа СЭУ (с двумя МОД) на судах меньшей грузовместимости (не позволяет ширина машинного отделения). Верхняя граница устанавливается теоретически, например, в [2] – на сегодняшний день нет более крупных СПГ-танкеров. Расчёты были проведены для плеча рейса в 3 тыс. морских миль и скорости хода в 19,5 уз. Интенсивность испарения груза (BOR) была принята минимально возможной для морских условий эксплуатации – 0,12% в сутки от полной грузовместимости. В качестве главных двигателей (ГД) были рассмотрены MAN B&W G60ME-GI [3] и G70ME-

GI [4]. Экономичность вспомогательных двигателей (ВД) – приводов электрогенераторов – принята на уровне Wärtsilä 34DF [5]. Результаты расчётов приведены на рис. 2, на котором левая часть неравенства (1) обозначена как $w_{распол}$, правая – $w_{ВД}$.

Из рис. 2 следует, что, во всём расчётном диапазоне, испаряющегося СПГ достаточно для питания как ГД, так и ВД; для супер-СПГ-танкеров характерна значительная избыточность испаряющегося газа – более 200 м^3 за рейс. Избыток испаряющегося газа может либо дожигаться, либо сжижаться повторно установкой повторного сжижения газа (УПСГ).

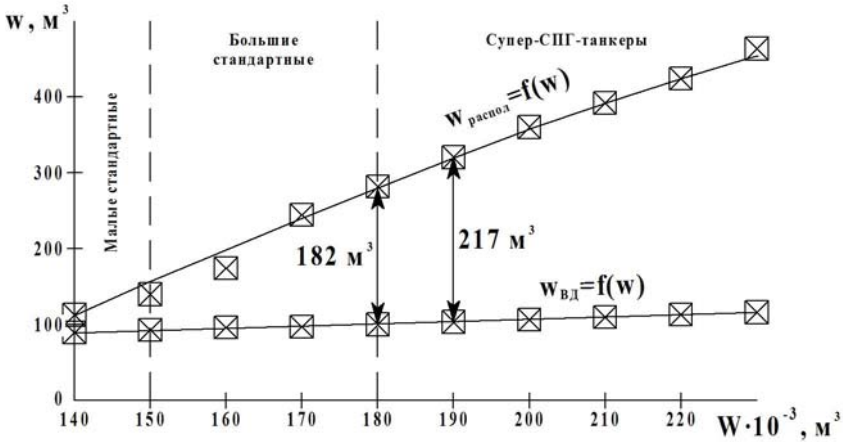


Рис. 2. Избыточность испаряющегося СПГ за рейс

Решение о применении УПСГ принимается для конкретного проекта судна исходя из прогнозируемой цены на СПГ. Для целей анализа граничное значение потерь газа, определяющее необходимость использования УПСГ, принято равным 200 м^3 за рейс. Стоимость этого объёма груза, например, исходя из цен на СПГ на азиатском рынке [6], составляет порядка 40 тыс. долл. США. Таким образом на малых и больших стандартных СПГ-танкерах с МОД достаточно в составе вспомогательной СЭС иметь двухтопливные электрогенераторные агрегаты и дожигать незначительный избыток испаряющегося газа. Далее анализируется состав СЭС СПГ-танкеров грузовместимостью более 180 тыс. м^3.

3. Генерирование электроэнергии посредством систем глубокой утилизации теплоты. Системы глубокой утилизации теплоты (СГУТ) используют для генерирования электроэнергии ресурс утилизации ГД – их выхлопные газы – и совершенно не потребляют топливо. СГУТ делятся на 3 типа по применяемым приводным двигателям: утилизационные паротурбогенераторы (УПТГ), газотурбогенераторы (УГТГ) и парогазотурбогенераторы (УПГТГ). УГТГ в качестве рабочей среды используют непосредственно выпускные газы ГД. УПТГ работают на перегретом паре, генерируемом в утилизационных котлах за счёт энергии выпускных газов. УПГТГ – это электрогенераторы, приводимые одновременно паровой и газовой турбинами (утилизационными). Особенности СГУТ:

– мощность СГУТ зависит от режима работы ГД;
– их мощность сокращается с увеличением общесудовой потребности в паре;
– применение самих СГУТ снижает экономичность ГД;
– УГТГ проще конструктивно, но при работе ГД на нефтяном топливе или топливной смеси с его высоким содержанием происходит интенсивное загрязнение газовой турбины продуктами сгорания и, как следствие, снижение её мощности;
– если газы от УГТГ затем направляются в утилизационный котёл, то первые реализуют сравнительно малый перепад давлений;
– применение УПТГ значительно усложняет схему СЭУ – необходим конденсатно-питательный контур;
– работа УПТГ на промежуточной среде – перегретом паре – исключает потерю мощности вследствие засорения проточной части турбины;
– применение промежуточной среды в УПТГ (водяного пара) приводит к дополнительным потерям энергии, вследствие которых мощность УПТГ всегда ниже, чем УГТГ.

На рис. 3 приведены графики изменения механической мощности СГУТ (УПГТГ) и УПСГ в относительных величинах (относительно эксплуатационной мощности СЭС) в зависимости от грузовместимости.

Из рис. 3 следует, что СГУТ не способны полностью обеспечить супер-СПГ-танкеры электроэнергией. Отклонения мощности СГУТ от линии тренда вызваны изменениями режима работы ГД. Также из рисунка видно, что недостающая доля электроэнергии всегда больше, чем мощность, необходимая для работы УПСГ. Т.е. СГУТ не способна обеспечить даже частично режимы работы УПСГ. Откуда следует, что, для обеспечения судна электроэнергией в достаточном количестве на ходовом режиме, СГУТ должна работать параллельно с электрогенераторными агрегатами других типов.

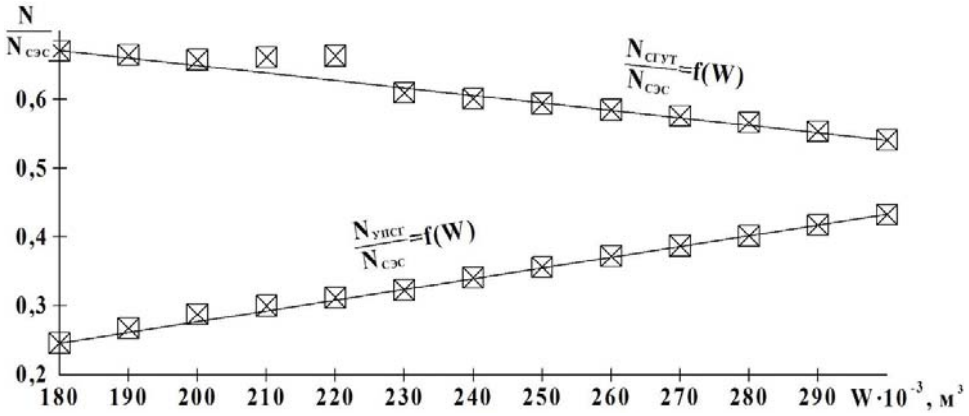


Рис. 3. Относительные мощности СГУТ и УПСГ

4. Применение валогенераторов в составе СЭУ СПГ-танкеров. Применение ВГ – это наилучшая из альтернатив при невозможности полного обеспечения судна электроэнергией СГУТ (с позиции минимизации числа одновременно работающих приводных двигателей). Особенности применения ВГ (в т.ч. параллельно со СГУТ):

– мощностью ВГ определяется эксплуатационный режим главных двигателей;

– для постоянного нахождения эксплуатационной точки ГД в пределах рабочего поля необходимо обеспечить примерно постоянную загрузку ВГ. Так, для работы УПСГ, имеющей переменную загрузку и высокую номинальную мощность, необходимо предусмотреть второй тип генераторов, работающих параллельно с ВГ (это может быть СГУТ либо ВД);

– электроэнергия, недостающая УПСГ, может быть получена СГУТ, но в этом случае СГУТ будет работать только в грузе;

– увеличение мощности ГД на величину мощности ВГ увеличивает ресурс утилизации, т.е. потенциальную мощность СГУТ;

– если СГУТ эксплуатируется параллельно с ВГ и обеспечивает только работу УПСГ, то её мощность, в ряде случаев, будет меньше максимально возможной (потенциальной).

На рис. 4 приведены графики изменения потенциальной мощности типов СГУТ, а также мощности, требуемой от них при условии, что ВГ обеспечивают электроэнергией всех потребителей кроме УПСГ ($N_{УПСГ} = N_{СЭС} - N_{ВГ}$) в зависимости от грузовместимости СПГ-танкера.

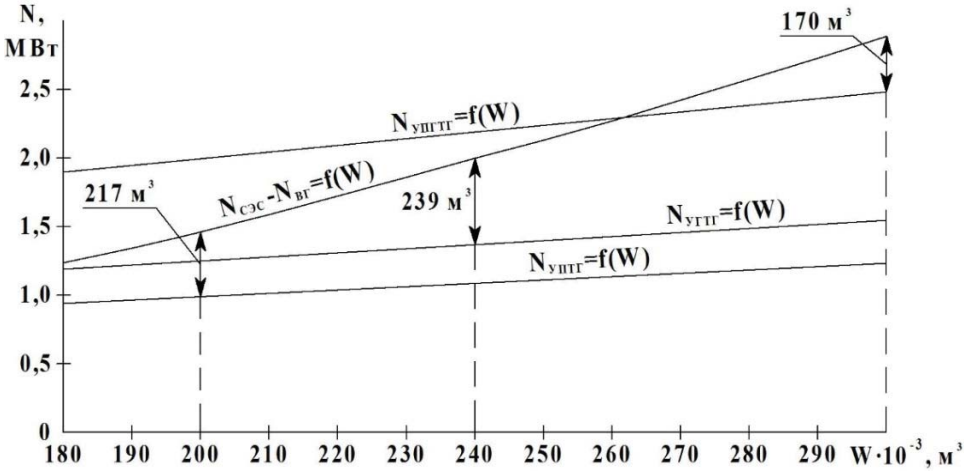


Рис. 4. Мощность СГУТ различных типов

Из рис. 4 следует, что потенциальные мощности УПТГ и УГТГ меньше максимально необходимых для УПСГ, т.е. недостающую мощность должны будут вырабатывать ВД, либо возможно частичное дожигание испаряющегося газа. В этих условиях УПТГ применимы на СПГ-танкерах грузовместимостью до 200 тыс. м^3, УГТГ – до 230-240 тыс. м^3. При большей грузовместимости единственный тип СГУТ, исключающий необходимость параллельной работы ВД, – это УПГТГ. Как видно из рис. 3, при грузовместимости до 260 тыс. м^3 УПГТГ способны полностью обеспечивать работу УПСГ. При большей грузовместимости потери газа за рейс не будут превышать 200 м^3 (либо, для исключения потерь, могут быть применены ВД).

На рис. 5 представлена гистограмма с характеристиками трёх вариантов комплектации СЭС СПГ-танкера грузовместимостью 260 тыс. м^3:

На ходовом режиме работают только двухтопливные вспомогательные двигатели;

Эти же ВД работают параллельно со СГУТ;

СГУТ работает параллельно с ВГ.

Сравниваемые характеристики: мощность СЭС на ходу ($N_{СЭС}$); конструктивный коэффициент энергетической эффективности (ККЭЭ, категория ледовых усилений – Ice 3) [7]; коэффициент полезного действия (КПД) СЭУ ($\eta_{СЭУ}$); среднечасовой расход СПГ ($B_{СПГ}$). В соответствии с рис. 5, наибольшую энергетическую эффективность обеспечивают схемы СЭС, включающие СГУТ, незначительно различающиеся по ККЭЭ и КПД СЭУ. Использование СГУТ параллельно с ВГ увеличивает среднечасовые затраты по топливу, т.к. сама СГУТ работает только при ходе в грузе, покрывая потребность УПСГ в электроэнергии.

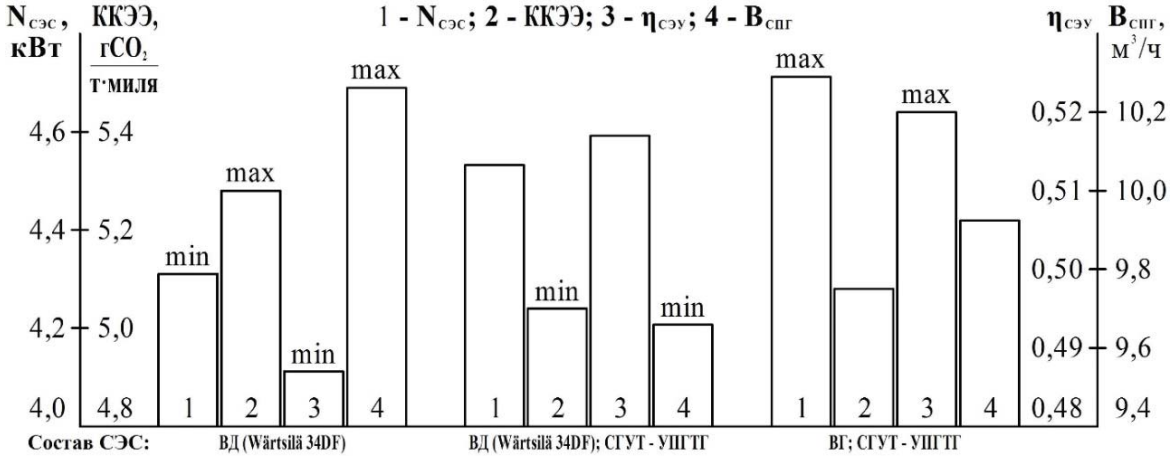


Рис. 5. Характеристики вариантов комплектации СЭС

Наименьшую экономичность имеет вариант с СЭС, оснащённой только двухтопливными ВД, т.к. ВД работают на испаряющемся СПГ (т.е. расходуют топливо/груз) и их экономичность ниже, чем у ГД. С другой стороны, малоэкономичные ВД позволяют уменьшить мощность УПСГ и, соответственно, мощность СЭС. Мощность СЭС максимальна у третьего варианта. Этому способствует высокая экономичность МОД, служащих приводами ВГ (увеличивается нагрузка на УПСГ), а также увеличение мощности топливных компрессоров высокого давления (пропорционально увеличению мощности МОД на величину мощности ВГ).

Изложенное позволяет сделать следующие выводы:

1. Наиболее остро вопрос оптимизации схем комплектации электростанций генераторными агрегатами стоит для СПГ-танкеров рефрижераторного типа с малооборотными ГД.

2. Ввиду того, что, среди существующих типов транспортных судов, СПГ-танкеры обладают сложным энергетическим комплексом, наиболее перспективным способом решения этой задачи следует считать использование современных технологий автоматизированного расчёта и инженерного анализа класса CAE, в том числе с применением программного комплекса «LNGC-PP».

3. Неоспоримое преимущество такого подхода заключается в решении ответственных и трудоёмких многовариантных оптимизационных задач итерационно – численными методами, в короткие сроки и с необходимым качеством (точностью и полнотой учета большого числа факторов). Тем более, в условиях отсутствия в настоящее время обобщенного решения данной оптимизационной задачи для СПГ-танкеров различных классов.

4. Предложен метод численного моделирования оценки и оптимизации комплектации СЭС СПГ-танкеров классов «Малый стандартный» и «Большой стандартный» электрогенераторами, приводимыми двухтопливными ВД.

5. Показано, что для супер-СПГ-танкеров является рациональным использование элементов систем глубокой утилизации теплоты параллельно с двухтопливными ВД, либо с ВГ.

6. Показана возможность широкого применения СГУТ типа УПГТГ, максимально эффективно утилизирующих теплоту выпускных газов ГД, что способствует сокращению потерь груза (СПГ) при транспортировке.

СПИСОК ЛИТЕРАТУРЫ

1. Р.О. Голубев. Система автоматизированного проектирования энергетической установки СПГ-танкера. // Сборник трудов. Региональная информатика и информационная безопасность. № 5, 2018. С. 466-470.
2. Propulsion Trends in LNG Carriers. – Копенгаген: MAN Diesel & Turbo, 2013. – 20 с.
3. MAN B&W G60ME-C9.5-GI-TII, Project Guide. – Копенгаген: MAN Diesel & Turbo, 2017. – 456 с.
4. MAN B&W G70ME-C9.5-GI-TII, Project Guide. – Копенгаген: MAN Diesel & Turbo, 2017. – 456 с.
5. WÄRTSILÄ 34DF, Product Guide. – Хельсинки: Wärtsilä, 2017. – 232 с.
6. 2018 World LNG Report. – Барселона: International gas union, 2018. – 106 с.
7. MARPOL 73/78 Annex 5, Resolution MEPC.245(66), Guidelines on the method of calculation of the attained EEDI for new ships. 2014. – 30 с.

УДК 004.514.6

КВАЛИМЕТРИЧЕСКОЕ РАНЖИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА MRP II ПРИ ПРОЕКТИРОВАНИИ «ОКЕАНИЧЕСКОЙ ТЕПЛОВОЙ ЭЛЕКТРОСТАНЦИИ»

Даулетьярова Назгуль Кайнаровна
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mail: nazgulya.d@mail.ru

Аннотация. Программное обеспечение для планирования производственных ресурсов при проектировании, называемое «Планирование требований к материалам» или MRP II, является основной технологией, которая используется при проектировании океанических и морских тепловых электростанций. При их проектировании реализуются задачи анализа и синтеза, оценки параметров основных процессов тепловой электростанции, прогнозирования динамики событий при получении электроэнергии. Для выбора лучших из возможных программных комплексов по технологии MRP II принципиально необходимо выполнять квалиметрическое их ранжирование с формированием соответствующих баз данных по их конкурентной способности и перспективности развития.

Ключевые слова: источник энергии; квалиметрия; ранжирование; конкурентная способность, океаническая тепловая электростанция.

QUALIMETRIC RANKING OF INFORMATION TECHNOLOGIES OF THE CLASS MRP II WHEN DESIGNING THE «OCEANIC HEAT ELECTRIC POWER STATION»

Dauletyarova Nazgul
St. Petersburg State Marine Technical University
3 Lotsmanskaya Str., St. Petersburg, 190121, Russia
e-mail: nazgulya.d@mail.ru

Abstract. Production resource planning software in design, called «material requirements Planning» or MRP II, is the core technology used in the design of ocean and marine thermal power plants. In their design, the tasks of analysis and synthesis, assessment of the parameters of the main processes of the thermal power plant, forecasting the dynamics of events in the production of electricity are implemented. In order to select the best of the possible software systems for MRP II technology, it is fundamentally necessary to perform their qualimetric ranking with the formation of appropriate databases on their competitive ability and prospects of development.

Keywords: energy source; qualimetry; ranging; competitive ability, ocean thermal power plant.

В свете происходящих событий, а именно бьющих все новые рекорды цен на нефть, всё больший интерес представляет освоение альтернативных источников энергии. Одним из наиболее привлекательных источников по количеству запасенной в нём энергии, является Мировой океан. А одной из наиболее перспективных технологий по извлечению скрытой в океане энергии являются морские и океанские (океанические) тепловые электростанции (ОТЭС) [1].

Основная идея океанической тепловой электростанции - извлечение энергии из перепада температур между теплыми поверхностными слоями и холодными глубинными слоями воды. Устойчивая разница температур в умеренной климатической зоне достигает на поверхности воды $T1=25^0$ и $T2=5^0$ на глубине порядка 500 м дает перепад температур 20^0, которой вполне достаточно для работоспособности ОТЭС.

ОТЭС, работающие по закрытому циклу, использует низкокипящее рабочее тело (аммиак или фреоны) которое испаряются в испарителе за счет подвода тепла от верхних слоев. Пары рабочего тела при повышенных температурах и давлении поступают в турбоагрегат, где вырабатывается электроэнергия. Из турбогенератора пары рабочего тела поступают в конденсатор, где они конденсируются, контактируя с водой, взятой из океанических глубин через трубопровод холодной воды. Далее рабочее тело подается в нагнетающий насос, откуда после повышения давления снова поступает в испаритель, замыкая термодинамический цикл [2].

При организационно-техническом проектировании ОТЭС закрытого цикла целесообразно использовать информационную технологию класса MRP II (планирование производственных ресурсов). Manufacturing Resource Planning, MRP II — метод, основанный на использовании планирования потребности в материалах, включающий в себя функции управления складами, снабжением, продажами и производством.

Принцип работы MRP II при проектировании ОТЭС опирается на три базовых принципа: иерархичность, интерактивность и интегрированность.

В соответствии с принципом иерархичности каждому звену производительной цепи присваивается свой уровень, совокупность которых образует иерархическую лестницу. Планирование проектирования ОТЭС осуществляется с высших ступеней. Одновременно с этим функционирует надёжный механизм обратной связи.

Интерактивность MRP II-системы обеспечивается заложенным в неё блоком моделирования. Суть интерактивности заключается в возможности анализа работы ОТЭС и прогнозирования развития событий при получении электроэнергии.

Интегрированность заключается в объединении множества сторон деятельности организации, среди которых планирование производства электроэнергии, снабжение производства, сбыт продукции, исполнение плана производства, учёт затрат и другие функции ОТЭС. Их основным содержанием является:

Планирование потребности в материалах, реализуемое подсистемой спецификаций (содержит нормативно-справочную информацию, необходимую для корректного планирования) и подсистемой операций с запасами (поддерживает в актуальном состоянии данные о запасах номенклатурных позиций).

Оперативное управление производством, при котором

– назначается способ расстановки приоритетов между руководящей и исполняющей сторонами,
– планируются потребности в мощностях.

Управление входным/выходным материальным потоком, при котором

– контролируется исполнение плана использования производственных мощностей.

Управление снабжением, при котором

– контролируется выполнение плана закупок и
– преобразуются заявки в заказы на закупку.

Планирование ресурсов распределения обеспечивается и в случае, когда предприятие имеет территориально распределённую структуру с несколькими удалёнными друг от друга площадками, реализуя:

– Закупки (Purchasing).
– Интерфейс с финансовым планированием.
– Оценку результатов деятельности (Performance Measurement).
– Моделирование (Simulation).

Одной из основных причин того, что MRP была с готовностью воспринята как методология управления производством, является ее обращение к возможностям вычислительной техники в области хранения и обработки больших массивов данных, предоставления доступа к ним в целях эффективного управления предприятием. Это помогает координировать деятельность различных подразделений при проектировании океанической тепловой электростанции.

Однако, различные варианты реализации возможностей технологии MRP II обладают далеко не одинаковым качеством, а выбор программного комплекса в этом классе только по критерию минимума стоимости владения (закупки, обслуживания, поддержки и т.п.) может оказаться даже ошибочным. Поэтому выбор лучшего из возможных программных комплексов, реализующего технологию MRP II, должен предворяться квалиметрическим их ранжированием с формированием соответствующих баз данных по их конкурентной способности и перспективности развития, т.е. количественной оценкой (измерением) их качества по соответствующим методикам, например, типа [4].

Более того, формирование и непрерывная актуализация соответствующих баз данных и знаний по каждому из классов подобных технологий, включая MRP II, а также по критериям их конкурентной способности и перспективности развития, позволит систематизировать важнейшие системные данные технологического их совершенствования, выполнять квалиметрическое ранжирование программных комплексов их реализации, что для практики проектирования имеет неоспоримое значение.

В условиях проектирования объектов морской техники на принципиально новой физической и технологической основе типа ОТЭС это одновременно позволит минимизировать проектные риски, исключить вероятность отказа от внедрения новых инновационных решений по причине неэффективной реализации пилотных проектов, что имеет особое значение для научно-технического прогресса и инвестиционной привлекательности новых направлений развития морской техники.

Вместе с тем, получаемые при этом квалиметрические оценки, инновационные результаты и показатели инвестиционной привлекательности должны быть максимально достоверными и самодостаточными. Это обязывает получающих и обеспечивающих эти оценки специалистов обладать достаточно высокими и разнообразными компетенциями, включая системотехнические знания, навыки и опыт, а передовые отрасли науки – своевременное создание и развитие соответствующих комплексных моделей и аппарата адекватного квалиметрического оценивания.

Выводы.

При проектировании и планировании производственных ресурсов новых, технологически революционных объектов, к числу которых в полной мере могут быть отнесены ОТЭС, должны максимально использоваться современные информационные технологии, включая MRP II («Планирование требований к материалам»).

При таком проектировании реализуются задачи максимально полного и качественного анализа и синтеза, и оценки параметров основных процессов океанических и морских тепловых электростанций, прогнозирования динамики событий при получении электроэнергии.

Для выбора лучших из возможных программных комплексов по технологии MRP II принципиально необходимо выполнять квалиметрическое их ранжирование с формированием соответствующих баз данных по их конкурентной способности и перспективности развития.

СПИСОК ЛИТЕРАТУРЫ

1. Борисёнок В., Соколов Б., Старостина В., Якобчук А. Минеральные богатства России и глобализация// Энергия: экономика, техника, экология. -2003. -.21-24.
2. World Energy Assessment: Energy and the Challenge of Sustainability. IIASA, 2002.
3. [Электронный ресурс] – Режим доступа: https://infopedia.su/3x6ae5.html свободный. – Загл. с экрана. (Дата обращения 10.11.2018)
4. Субетто А.И., Алексеев А.В. Теория практики квалиметрического обеспечения развития морских автоматизированных систем / Актуальные проблемы морской энергетики: материалы седьмой Всероссийской межотраслевой научно-технической конференции в рамках Второго Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2018, с. 78 – 86.

УДК 378.147:378.018.43; 519.872; 519.873

ОБОСНОВАНИЕ ЦЕЛЕСООБРАЗНОСТИ И СПОСОБА ВВЕДЕНИЯ В ОЛВМ ЛОГИЧЕСКОЙ ОПЕРАЦИИ «ПРИОРИТЕТ»

Можаева Ирина Александровна[1], Поленин Владимир Иванович[2], Струков Александр Владимирович[1], Сущенков Дмитрий Андреевич[2]

[1] АО «СПИК СЗМА»
26-я линия В.О., 15 стр.2А, Санкт-Петербург, 199106, Россия
[2] Военный учебно-научный центр Военно-Морского флота «Военно-Морская академия им. Н.Г. Кузнецова»
Ушаковская наб., 17, Санкт-Петербург, 197045, Россия
e-mails: irgladkova@gmail.com, alexander_strukov@szma.com, polenin@mail.ru, sushenkov_dmitri@mail.ru

Аннотация. Рассматривается целесообразность и технология введения в ОЛВМ и ПК АСМ операции «Приоритет» в целях обеспечения адекватного модельного отображения последовательности наступления событий в процессах функционирования технических систем и вооруженной борьбы. Приводятся модульные решения задачи в форме схем функциональной целостности ОЛВМ или, что то же, ориентированных логико-вероятностных графов функционирования систем. Дается математический аппарат вычисления логико-вероятностных функций, соответствующих логической операции «Приоритет».

Ключевые слова: ориентированные логико-вероятностные графы; модели функционирования; технические системы; вооруженная борьба; последовательность наступления событий.

JUSTIFICATION OF VALIDITY AND METHOD OF INTRODUCTION OF THE LOGIC OPERATION «PRIORITY»

Mozhaeva Irina [1], Polenin Vladimir [2], Strukov Alexander [1], Suuschenkov Dmitry [2]

[1] JSC «SPIK SZMA»
15/2a 26th liniya, Vasilievsky Island, St. Petersburg, 199106, Russia
[2] Military training and research center of the Navy «Naval Academy named after N. G. Kuznetsov»
17 Ushakovskaya Emb., St. Petersburg, 197045, Russia
e-mails: irgladkova@gmail.com, alexander_strukov@szma.com, polenin@mail.ru, sushenkov_dmitri@mail.ru

Abstract. The feasibility and technology of introducing the “Priority” operation into the OLMM and the ASM PC are considered in order to ensure an adequate model display of the sequence of occurrence of events in the processes of operation of technical systems and warfare. Modular solutions of the problem are given in the form of schemes of functional integrity of the OLVM or, what is the same, oriented logical-probabilistic graphs of the functioning of systems. The mathematical apparatus for calculating the logical-probabilistic functions corresponding to the logical operation «Priority» is given.

Keywords: oriented logical-probabilistic graphs; functioning models; technical systems; armed struggle; sequence of occurrence of events.

1. Постановка задачи. Практика моделировании функционирования технических систем и вооруженной борьбы показывает, что иногда процесс их функционирования необходимо отобразить с учетом наступления некоторых событий в заданной последовательности.

Пусть, например, фрагмент СФЦ моделируемой системы имеет вид, приведенный на рис. 1.

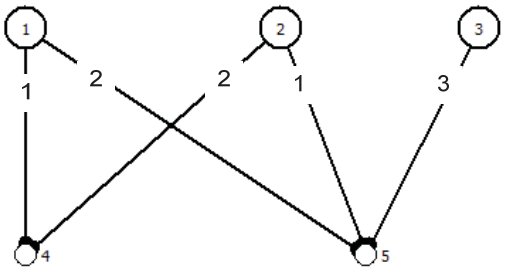


Рис.1. Фрагмент СФЦ моделируемой системы

По смыслу процесса функционирования системы событие 4 должно наступать при осуществлении исходных событий 1 и 2 в последовательности 1→2, а событие 5 – при осуществлении исходных событий 1, 2 и 3 в последовательности 2→1→3.

Отображение такого рода последовательностей наступления событий с применением базиса логических операций «И», «ИЛИ», «НЕ» недоступно.

Возникает необходимость дополнения этого базиса операцией «Приоритет», которая основана на операции «И» с дополнительным указанием заданной последовательности наступления исходных событий группы, к которой применяется операция «И».

Общий случай наступления в заданной последовательности наступления некоторой совокупности $n>2$ исходных событий является проблематичным как в теоретическом решении, так и в реализации в программных комплексах ОЛВМ. Ниже на наглядном примере дуэли рассматривается достаточный для большинства практических задач моделирования функционирования технических систем и вооруженной борьбы вариант с двумя исходными событиями.

2. Схема развития дуэли с учетом упреждающих и ответных ударов. Применительно к вооруженной борьбе этот вариант необходим и достаточен для модельного отображения боевого столкновения двух боевых систем или тактических единиц в форме обмена ударами.

Важнейшими факторами, определяющими исход противоборства, являются характеристики упреждений в ударах сторон и потенциалы (вероятности) поражения противника.

Пусть удары сторон будут поражающими, то есть, если какой-либо удар состоялся, то это означает поражение противника. Поскольку речь идет о некотором модельном модуле, типовом элементе моделей вооруженной борьбы, которые предстоит создавать пользователю, этому типовому модулю необходимо придать строгость оформления. Для формализованных моделей условием выполнения строгости является адекватность модели реальным закономерностям вооруженной борьбы.

Первое условие адекватности отображения исхода вооруженного противоборства по последовательности выполнения поражающих ударов сторонами состоит в том, что исходные события образуют полную группу несовместных событий (рис. 2):

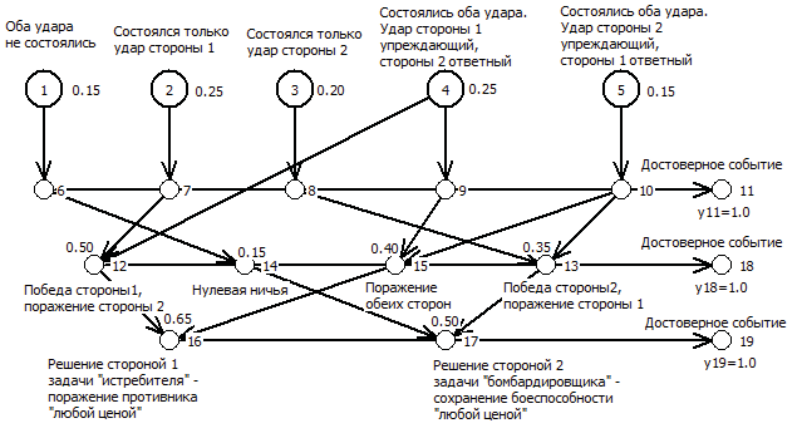


Рис. 2. Событийные варианты обмена ударами в дуэли

В приводимой СФЦ достоверные события являются суммами: событие 11 является суммой событий 6 – 10, событие 18 – суммой событий 12 – 15, событие 19 – суммой событий 16, 17. Горизонтальное проведение связей «ИЛИ» значительно упрощает СФЦ и облегчает ее восприятие.1 – оба удара не состоялись;

Отдельные события:

2 – состоялся только удар стороны 1;

3 – состоялся только удар стороны 2;

4 – состоялись оба удара: удар стороны 1 упреждающий, стороны 2 ответный;

5 – состоялись оба удара: удар стороны 1 упреждающий, стороны 2 ответный.

Заметим, что если удары ответно-встречные, то есть события 4 и 5 состоят в том, что состоялись оба удара, но один из них произведен раньше другого, то формально, по последствиям, эти события неразличимы и их следует объединить в одно событие: «состоялись оба удара, при этом один из них выполнен раньше другого».

Второе условие адекватности состоит в том, что эти исходы должны образовывать полную группу несовместных событий, то есть сумма вероятностей их наступления должна равняться 1.0. Признак несовместности задается пользователем с помощью интерфейса программного комплекса, а выполнение условия полной группы обеспечиваются точным равенством суммы вероятностей в вершинах 1 – 5 значению 1.0.

Дальнейшее объединение производных событий в итоговые, интересующие пользователя, порождается интуитивной логикой. Можно видеть, что свойство полноты групп событий соблюдается во всех исходных, промежуточных и итоговых группах событий.

Здесь следует обратить внимание на то обстоятельство, что внешне условие нормировки по группам событий несовместных событий 12 – 15 и 16, 17 не выполняется. Хотя с помощью программного комплекса на выходах вершин 18 и 19 получается значение 1.0, внешне просчитываемая сумма вероятностей событий 12 – 15 составляет 0.50+0.15+0.40+0.35=1.40, что является грубой ошибкой. Вместе с тем, здесь никакой ошибки нет. Дело в том, что в состав суммы событий 12 – 15 значения вершин 4 и 5 входят дважды. Согласно закону идемпотентности [2], при многократном суммировании или перемножении событий они учитываются в результатах лишь однократно. При этом можно видеть, что условие нормировки выполняется точно.

Таким образом, набор исходных событий вида 1 – 5 полностью удовлетворяет требованиям как решения задачи пользователя, так и условия адекватности модели.

Данный вариант формирования модели дуэльного противоборства сторон неудобен в связи с тем, что значения исходных вероятностей наступления событий 1 – 5 нужно рассчитывать и задавать вне программного комплекса.

Рассматриваемая технология моделирования вооруженной борьбы с учетом факторов упреждений в ударах сторон разработана и опубликована в монографии [2]. А.С. Можаев реализовал эту технологию в одном из вариантов ПК АСМ 2001 путем выделения пяти специализированных функциональных вершин с зарезервированными номерами 900, 910, 920, 912, 921, содержащих расчетные значения вероятностей всех возможных вариантов последовательностей нанесения ударов противоборствующих сторон:

- 900 – удары сторон не состоялись;
- 910 – состоялся только удар стороны 1;
- 920 – состоялся только удар стороны 2;
- 912 – состоялись оба удара: упреждающий удар стороны 1, ответный удар стороны 2;
- 921 – состоялись оба удара: упреждающий удар стороны 1, ответный удар стороны 2.

Эта технология демонстрируется ниже (рис. 3).

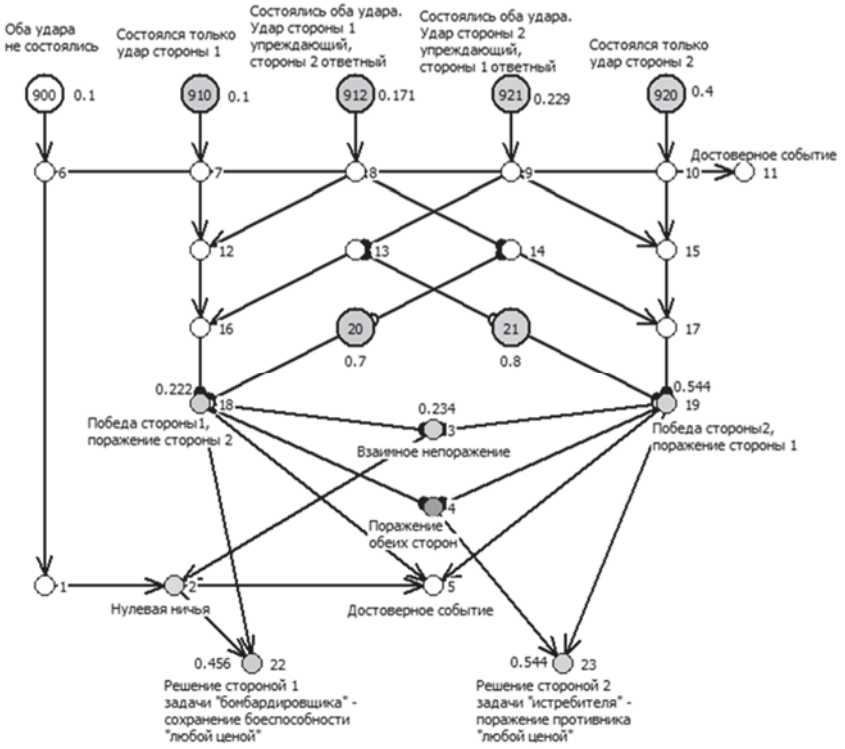


Рис.3. СФЦ моделирования дуэли с использованием пяти событийных вершин по вариантам развития дуэли

Однако ограниченность моделирования только пятью вершинами с заблаговременно зарезервированными для них номерами позволяет моделировать боевые столкновения лишь одиночной дуэли, не допуская возможности моделирования множественных обменов ударами.

Возможный путь преодоления этих недостатков представлен теорией развития и исхода противоборства типа дуэли в монографии [2] в §5.4 «Вероятностная оценка исходов дуэли с учетом последовательностей нанесения ударов (действий)» и в статье [3].

Однако, как реализовать этот способ в теории ОЛВМ и в программном коде ПК АСМ, оставалось неясным. Очевидно было лишь то, что применение для этого полного базиса логических операций «И», «ИЛИ», «НЕ» является недостаточным.

Впоследствии, в ходе работ по совершенствованию технологии моделирования вооруженной борьбы был найден способ обеспечения возможности множественного моделирования обмена ударами. Этот способ заключался в применении, наряду с логическим базисом операций «И», «ИЛИ», «НЕ», дополнительной логической операции «Упреждение» или «Раньше» [1].

Ниже рассматривается вариант такой реализации с помощью дополнительной логической операции «Приоритет».

3. Модель дуэли с использованием логической операции «Приоритет». Важнейшими факторами, определяющими исход противоборства, являются характеристики упреждений в ударах сторон и потенциалы (вероятности) поражения противника. Чтобы не переусложнялась СФЦ дуэли, целесообразно считать, что нанесение удара сопровождается поражением цели.

В модели статических расчетов это достигается формированием вероятностей, рассчитанных так, чтобы они одновременно отражали влияние факторов и упреждения, и поражения. В модели вероятностно-временных

расчетов следует сформировать функции распределения моментов времени нанесения поражающих ударов и придать им вес вероятностного потенциала поражения (рис. 4).

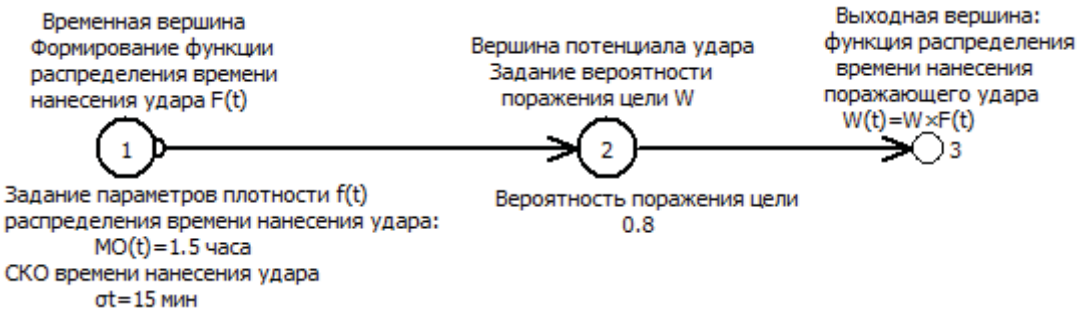


Рис.4. Формирование функции распределения момента времени нанесения поражающего удара

Требуется обеспечить моделирование развития дуэли уже не с заданием, а с расчетным формированием пяти вариантов исходов эпизода обмена ударами (рис. 2) с использованием модуля рис. 1 и логической операции «Приоритет» (рис. 1). СФЦ, обеспечивающая это моделирование, представлена на рис. 5.

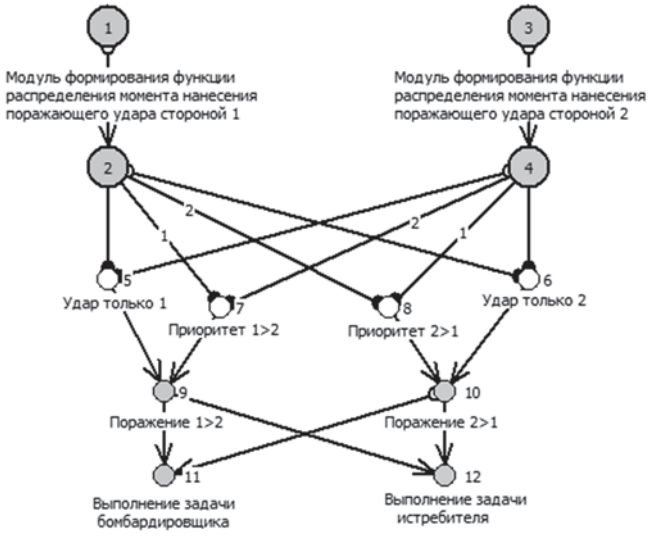


Рис. 5. СФЦ дуэли с использованием модулей формирования функций распределения моментов времени нанесения поражающих ударов и логической операции «Приоритет»

Применение этой типовой, модульной СФЦ позволяет осуществлять моделирование одновременно множества дуэлей.

4. Расчетное обеспечение логической операции «Приоритет». Имея заданные плотности распределения моментов времени ударов $f_1(t)$ и $f_2(t)$, можно получить аналитические формулы для вычисления вероятностей соответствующих событий – вариантов обмена ударами в функции текущего времени дуэли.

Ниже приводятся формулы для вычисления вероятностей осуществления событий в приоритетной последовательности.

Вариант 1->2 – по приоритету событие 1 наступает раньше, чем событие 2:

$$P_{1->2}(t)=\int_0^t f_x(x)dx\int_x^t f_y(y)dy=\int_0^t\left[F_y(t)-F_y(x)\right]f_x(x)dx=$$
$$=\int_0^t f_y(y)dy\int_0^y f_x(x)dx=\int_0^t\left[F_x(y)-F_x(0)\right]f_y(y)dy. \quad (1)$$

Вариант 2->1 – по приоритету событие 2 наступает раньше, чем событие 1:

$$P_{2->1}(t)=\int_0^t f_y(y)dy\int_y^t f_x(x)dx=\int_0^t\left[F_x(t)-F_x(y)\right]f_y(y)dy=$$
$$=\int_0^t f_x(x)dx\int_0^x f_y(y)dy=\int_0^t\left[F_y(x)-F_y(0)\right]f_x(x)dx. \quad (2)$$

Достоверность результатов подтверждается в монографии [2] и публикациях [1, 2].

В целом представляется возможным утверждать, что:

Введение в теорию ОЛВМ и в программный код ПК АСМ двух операций (1) и (2) вычислений и нумерованных стрелок согласно приоритетов проблемным не является;

Реализация операции «Приоритет» обеспечит возможность адекватного моделирования функционирования технических систем и вооруженного противоборства с обменом сторонами ударами во множестве дуэльных эпизодов.

СПИСОК ЛИТЕРАТУРЫ

1. Вероятностная оценка текущей и итоговой устойчивости боевых и технических систем в условиях воздействия поражающих факторов с применением ОЛВМ/ В.И. Поленин, И.А. Можаева, А.А. Потехин, Д.А. Сущенков // XIV Санкт-петербургская международная конференция «Региональная информатика (РИ-2016)». – СПб, 27-29 октября 2016 г.
2. Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженной борьбы // Монография, научное издание / В.И. Поленин, И.А. Рябинин, С.К. Свирин, И.А. Гладкова. Под ред. А.С. Можаева. – СПб: СПб-региональное отделение РАЕН, 2011.
3. Применение теории вероятностей в событийных моделях вооруженного противоборства / В.И. Поленин, А.С. Можаев, И.А. Гладкова. – Морская радиоэлектроника, №4 (46), декабрь 2013.

УДК 004.75

ОБЕСПЕЧЕНИЕ СЕТЕВОЙ ОТКАЗОУСТОЙЧИВОСТИ И БАЛАНСИРОВКИ НАГРУЗКИ В РАСПРЕДЕЛЕННЫХ КОРАБЕЛЬНЫХ СИСТЕМАХ УПРАВЛЕНИЯ

Носков Илья Игоревич
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: noskovii@mail.ru

Аннотация. Проанализированы проблемы обеспечения отказоустойчивости и балансировки нагрузки в современных распределенных корабельных системах управления. Рассмотрен протокол обеспечения сетевой отказоустойчивости и балансировки нагрузки GLBP. Предложен метод разработки моделей распределенных систем управления в среде OMNeT++.

Ключевые слова: отказоустойчивость; балансировка нагрузки; GLBP; компьютерное моделирование; корабельные системы управления; компьютерные сети; OMNeT++.

PROVIDING FAULT-TOLERANCE OF NETWORK AND LOAD BALANCING FOR DISTRIBUTED MARINE CONTROL SYSTEMS

Noskov Ilya
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (University ITMO)
49 Kronverksky Av., St. Petersburg, 197101, Russia
e-mail: noskovii@mail.ru

Abstract. Fault-tolerance and load balancing problems in modern distributed marine control systems are analyzed. Gateway load balancing protocol is considered. The paper describes the method of developing distributed control systems models in OMNeT++.

Keywords: fault-tolerance; load balancing; GLBP; computer simulation; marine control systems; computer networks; OMNeT++.

Введение.

Современные системы управления, в число которых входят и корабельные, строятся на базе распределенных вычислительных систем. Такие распределенные системы включают в себя вычислительные узлы и коммуникационную среду, обеспечивающую взаимодействие между узлами. Для решения задач реального времени система управления должна быть производительной и обеспечивать высокий уровень отказоустойчивости [1], живучести [2-4], безопасности [5-6] надежности [7-8]. Обеспечение высокой надежности распределенных систем управления требует резервирования активного коммуникационного оборудования, выполняющего задачу связи и взаимодействия элементов и вычислительных устройств в системе [9-11]. Современное сетевое оборудование позволяет передавать данные между вычислительными узлами на достаточно больших скоростях. В корабельных системах управления при отказах сетевого оборудования очень быстро теряется актуальность передаваемых данных и нарушается процесс управления судном, что может повлечь за собой достаточно серьезные последствия. В связи с чем возрастает потребность в построении отказоустойчивых систем управления, предоставляющих свои услуги с минимальной задержкой даже при отказе одного из элементов. Для обеспечения отказоустойчивости активного сетевого оборудования, входящего в состав корабельной системы управления, разработано семейство протоколов FHRP (First Hop Redundancy Protocols), позволяющее объединять оборудование в группу, тем самым увеличивая отказоустойчивость системы в целом, т.к. отказоустойчивость группы сетевого оборудования выше, чем отказоустойчивость каждого отдельного ее элемента. Для исследования и оценки работы различных протоколов семейства FHRP [12-14] подходит

имитационное моделирование, которое позволяет строить модели систем и исследовать их без необходимости построения компьютерных сетей из реального оборудования.

Основными реализациями семейства протоколов FHRP являются: VRRP, HSRP и GLBP [12,15,16]. Моделирование и изучение работы данных протоколов поможет выявить преимущества и недостатки той или иной реализации, чтобы в дальнейшем применить один из данных алгоритмов в реализации распределенной отказоустойчивой корабельной системы управления. В настоящее время средство моделирования компьютерных сетей OMNeT++ является узкоспециализированной кроссплатформенной средой, позволяющей строить модели компьютерных сетей различного уровня с использованием большого количества протоколов и технологий. Данная среда имеет богатую библиотеку сетевых компонентов, разработанных на языке C++, графический интерфейс пользователя, позволяющий быстро и удобно строить сетевые модели, а также подробную англоязычную документацию [17]. Среда предоставляет встроенный синтаксис языка описания компьютерных сетей NED, благодаря которому можно достаточно просто конфигурировать элементы сетевой архитектуры, разрабатываемой модели. На рис. 2 приведен фрагмент синтаксиса описания модели компьютерной сети с использованием языка NED:

```
    Host1: ANSA_Host {
        @display("p=150,250");
        gates:
            ethg[1];
    }
    Host2: ANSA_Host {
        @display("p=350,250");
        gates:
            ethg[1];
    }
connections:
    Host1.ethg[0] <--> Eth100M <--> SW1.ethg[2];
    Host2.ethg[0] <--> Eth100M <--> SW2.ethg[2];
```

Рис. 2. Описание модели компьютерной сети языком NED

В данном фрагменте конфигурационного файла указаны параметры хостов, а именно координаты расположения в графическом редакторе и количество сетевых интерфейсов, а также сконфигурированы сами соединения. В случае соединений (connections) описывается какие сетевые интерфейсы моделируемых устройств соединены между собой, дополнительно указывается пропускная способность каждого из каналов. Изменения, вносимые в конфигурационный файл сети NED отражаются на графическом представлении, что справедливо и в обратную сторону. На рис. 3 изображена графическая схема сети, позволяющая визуально представлять моделируемую сеть:

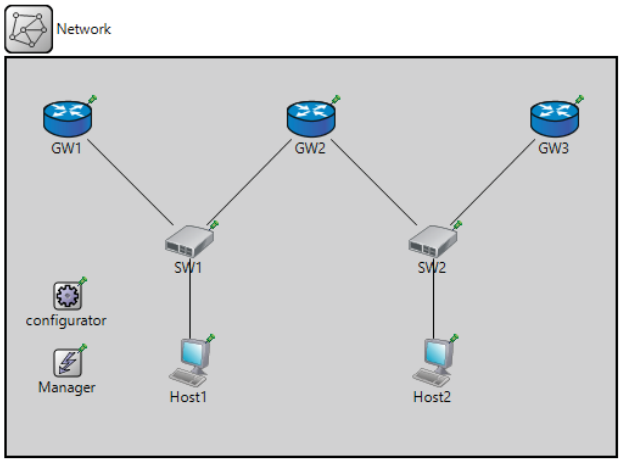


Рис. 3. Графический редактор построения моделей компьютерных сетей

Для среды моделирования OMNeT++ в настоящее время разрабатывается достаточно большое количество библиотек с моделями сетевых компонентов и протоколов взаимодействия между ними. Основной библиотекой с открытым исходным кодом, поддерживаемой разработчиками среды моделирования, является INET Framework. В данной библиотеке разработаны модели протоколов различных уровней стека OSI: канального (PPP, Ethernet, IEEE 802.11 и т.д.), сетевого (IPv4, IPv6, OSPF и т.д.), транспортного (TCP, UDP) [12]. Другой важной и полезной библиотекой является ANSAINET, которая расширяет библиотеку INET Framework дополнительными реализациями различных протоколов: разработаны модели протоколов обеспечения сетевой отказоустойчивости, алгоритмы динамической маршрутизации, протоколы маршрутизации мультикаста и т.д. Для моделирования работы протоколов обеспечения сетевой отказоустойчивости в ANSAINET разработаны модели маршрутизаторов, реализующие функционал данных протоколов: ANSA_VRRP_Router, ANSA_HSRP_Router и ANSA_GLBP_Router.

Протоколы семейства FHRP реализуют механизмы сетевой отказоустойчивости в современных компьютерных сетях путем обеспечения высокой доступности шлюзов, заданных по умолчанию, за счет их дублирования и совместной работы, а также гарантируют очень быстрое время восстановления в случае аварий. В рамках работы данных протоколов маршрутизаторы объединяются в так называемую «виртуальную группу», которой назначается один «виртуальный» IP-адрес. Таким образом, в каждый момент времени клиенты работают только с одним маршрутизатором из группы. При отказе основного маршрутизатора всю работу по обслуживанию клиентов берет на себя резервный маршрутизатор, причем для клиентов это делается абсолютно прозрачно, т.к. виртуальный адрес остается тот же, хотя трафик от клиента будет идти уже через другое физическое устройство.

Протокол GLBP (Gateway Load Balancing Protocol) как и другие протоколы семейства FHRP (VRRP, HSRP) выполняет резервирование маршрутизатора путем его дублирования другими устройствами и объединения их в группу. Однако возможности данного протокола не ограничиваются вариантом его использования в качестве протокола резервирования и обеспечения отказоустойчивости шлюза по умолчанию. Так как протоколы семейства FHRP создают виртуальную группу маршрутизаторов с одним общим виртуальным IP-адресом, в которую входят реальные физические маршрутизаторы и выбирают активным маршрутизатором только один из всей группы, то остальные маршрутизаторы остаются неактивными до тех пор, пока не случится сбой активного маршрутизатора и не произойдет выбор нового устройства из резервных, которое будет обрабатывать трафик, направленный на IP-адрес виртуальной группы. Данный подход обладает явными недостатками, т.к. происходит простой ресурсов резервных маршрутизаторов, которые не используются в течение времени эксплуатации системы пока не произошел отказ основного устройства. Преимуществом протокола GLBP является обеспечение распределения нагрузки между маршрутизаторами путем назначения им различных виртуальных MAC-адресов и одного виртуального IP-адреса, при этом все маршрутизаторы виртуальной группы участвуют в передаче пакетов [14]. GLBP может работать в нескольких режимах [15]:

– None – режим, при котором коммутатор не обеспечивает балансировку нагрузки и работает по сути, как все остальные протоколы семейства FHRP;

– Weighted load-balancing – балансировка нагрузки производится в соответствии с весом каждого устройства;

– Host-dependent load-balancing – используется при необходимости реализации технологии трансляции сетевых адресов (NAT);

– Round-robin load-balancing – в этом режиме маршрутизатор выполняет балансировку нагрузки и выдает MAC-адреса для членов группы попеременно.

Данные особенности протокола GLBP являются полезными для распределенных корабельных систем управления, так как помимо обеспечения отказоустойчивости сетевой подсистемы обеспечивается также распределение нагрузки по маршрутизаторам виртуальной группы. Распределение нагрузки позволяет ускорить процесс обработки и передачи трафика между узлами сети, что является полезным свойством в системах реального времени, таких как системы управления кораблем, где важна скорость и оперативность передачи данных.

Разработаем модель распределенной корабельной системы управления, состоящей из двух хостовых машин, на которых идет обработка данных, полученных с датчиков и посылаются сигналы управления, одного коммутатора, объединяющего данные машины в локальную сеть и трех маршрутизаторов, на которых запущен протокол GLBP для обеспечения отказоустойчивости и распределения нагрузки по остальным маршрутизаторам виртуальной группы. Для этого создадим новый проект в среде OMNeT++ и в редакторе сетевых моделей добавим 3 отказоустойчивых маршрутизатора со встроенным протоколом GLBP, один коммутатор и 2 хостовые машины. Соединим все устройства каналами связи. На рис. 4 изображена разработанная в графическом редакторе модель данной системы:

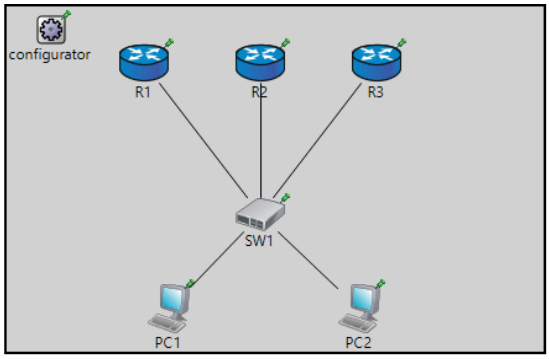


Рис. 4. Модель распределенной системы управления с отказоустойчивым шлюзом

Промоделируем ситуацию выбора главного активного виртуального шлюза для группы, который будет назначать виртуальные адреса для остальных маршрутизаторов группы. Для этого в конфигурационном файле модели зададим для маршрутизаторов одинаковый идентификатор виртуальной группы и виртуальный IP-адрес, также зададим маршрутизаторам одинаковый приоритет, чтобы активный виртуальный маршрутизатор был

выбран в автоматическом режиме (при одинаковых значениях приоритета активным выбирается маршрутизатор с наибольшим IP-адресом). На рис. 5 приведен фрагмент конфигурации маршрутизаторов:

```
<Devices>
    <!--    R1      -->
    <Router id="R1">
        <Interfaces>
            <Interface name="eth0">
                <IPAddress>192.168.1.1</IPAddress>
                <Mask>255.255.255.0</Mask>
                <GLBP>
                    <Group id="0" ip="192.168.1.254" priority = "100"></Group>
                </GLBP>
            </Interface>
        </Interfaces>
    </Router>

    <!--    R2      -->
    <Router id="R2">
        <Interfaces>
            <Interface name="eth0">
                <IPAddress>192.168.1.2</IPAddress>
                <Mask>255.255.255.0</Mask>
                <GLBP>
                    <Group id="0" ip="192.168.1.254" priority = "100"></Group>
                </GLBP>
            </Interface>
        </Interfaces>
    </Router>
```

Рис. 5. Конфигурация маршрутизаторов модели компьютерной сети

После разработки модели и запуска самого процесса моделирования в реальном времени можно отслеживать временную шкалу событий системы моделирования и процесс передачи пакетов и взаимодействия устройств между собой. На рис. 6 приведен скриншот процесса моделирования разработанной модели:

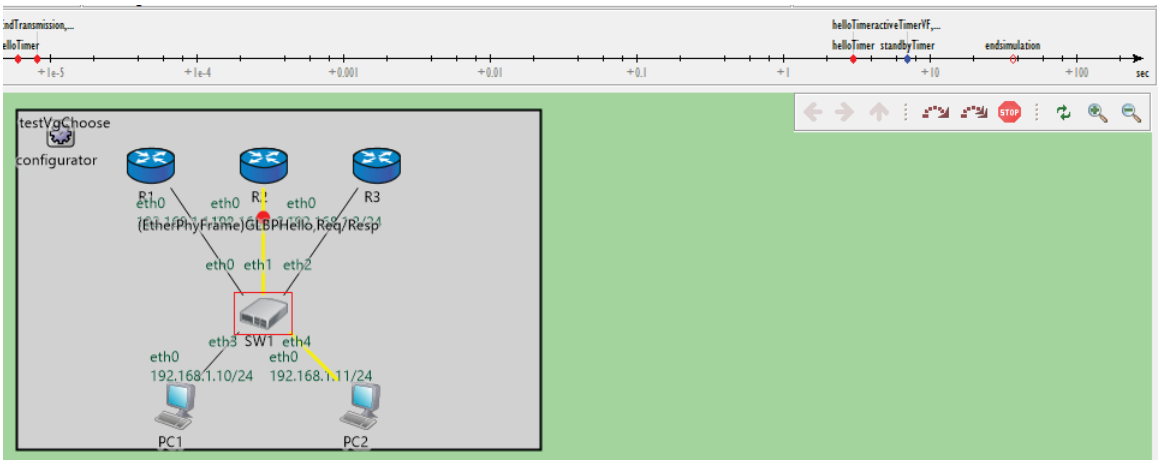


Рис. 6. Моделирование работы компьютерной сети

После выполнения процесса моделирования пользователю становятся доступны результаты в виде точной детализации всех событий с временными отметками и визуальной схемой, а также статистика по всем элементам моделируемой системы с возможностью построения различных диаграмм и графиков.

Из лога событий, полученного в результате моделирования можно увидеть, как маршрутизаторы обмениваются Hello-сообщениями, а также ARP-запросы, на который отвечает маршрутизатор R3. Лог событий процесса моделирования представлен на рис. 7:

Event#	Time	Src/Dest	Name	Info
#1181	20.00000853	SW1 --> R2	GLBPHello	inet::GLBPMessage:40 bytes
#1211	20.00001605	SW1 --> R3	GLBPHello	inet::GLBPMessage:40 bytes
#1212	20.00001605	SW1 --> PC1	GLBPHello	inet::GLBPMessage:40 bytes
#1213	20.00001605	SW1 --> PC2	GLBPHello	inet::GLBPMessage:40 bytes
#1230	20.00001701	SW1 --> R1	GLBPHello,Req/Resp	inet::GLBPMessage:60 bytes
#1231	20.00001701	SW1 --> R2	GLBPHello,Req/Resp	inet::GLBPMessage:60 bytes
#1252	20.00002453	SW1 --> PC1	GLBPHello,Req/Resp	inet::GLBPMessage:60 bytes
#1253	20.00002453	SW1 --> PC2	GLBPHello,Req/Resp	inet::GLBPMessage:60 bytes
#1290	20.00002618	R1 --> SW1	arpREQ	ARP req: 192.168.1.3=? (s=1
#1291	20.00002618	R2 --> SW1	arpREQ	ARP req: 192.168.1.3=? (s=1
#1303	20.00003199	SW1 --> R3	arpREQ	ARP req: 192.168.1.3=? (s=1
#1312	20.00003295	SW1 --> R1	arpREQ	ARP req: 192.168.1.3=? (s=1
#1313	20.00003295	SW1 --> R2	arpREQ	ARP req: 192.168.1.3=? (s=1
#1324	20.00003461	SW1 --> PC1	arpREQ	ARP req: 192.168.1.3=? (s=1
#1325	20.00003461	SW1 --> PC2	arpREQ	ARP req: 192.168.1.3=? (s=1
#1335	20.0000378	R3 --> SW1	arpREPLY	ARP reply: 192.168.1.3=0A-A

Рис. 7. Лог событий процесса моделирования

Таким образом, была промоделирована работа протокола GLBP, который может быть использован в построении отказоустойчивых распределенных корабельных систем управления. После проведения эксперимента пользователю становится также доступна детальная статистическая информация по всем компонентам, участвующим в процессе моделирования. На рис. 8 изображен фрагмент результатов моделирования для компонента канального уровня интерфейса eth0 маршрутизатора R3:

Name	Value
testVgChoose.R3.eth[0].mac	
bits/sec rcvd (scalar)	611.73333333333
bits/sec sent (scalar)	327.46666666667
droppedPkBitError:count (scalar)	0.0
droppedPkBitError:sum(packetBytes) (scalar)	0.0
droppedPkIfaceDown:count (scalar)	0.0
droppedPkIfaceDown:sum(packetBytes) (scalar)	0.0
droppedPkNotForUs:count (scalar)	0.0
droppedPkNotForUs:sum(packetBytes) (scalar)	0.0
frames/sec rcvd (scalar)	0.8
frames/sec sent (scalar)	0.43333333333333

Рис. 8. Результаты моделирования компонента компьютерной сети

На основе векторных данных, полученных в результате процесса моделирования, пользователю доступно построение различных графиков и гистограмм.

Заключение.

Разработан метод проведения имитационного эксперимента работы протокола обеспечения сетевой отказоустойчивости GLBP в среде OMNeT++ с использованием библиотеки INET и ANSAINET. Описаны основные этапы создания модели компьютерной сети и самого процесса моделирования. Использование данного подхода в дальнейшем позволит проводить эксперименты по изучению и исследованию особенностей протокола GLBP для возможности улучшения его характеристик и проектировать отказоустойчивые распределенные системы управления.

Представляет интерес развитие предлагаемых моделей в направлении построения систем реального времени критичных к задержкам обслуживания запросов, в которых вероятность своевременного обслуживания запросов достигается на основе распределения [18-19] и резервирования запросов с обслуживания их копий в разных серверах [20-21] и передаче запросов или их перераспределении через сеть по разным маршрутам [22].

СПИСОК ЛИТЕРАТУРЫ

1. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза. Ульяновск. Областная типография «Печатный двор» 2016 -544 с.
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. Смольников А.В. Алексеев А.В. Квалиметрическое обеспечение повышения конкурентоспособности объектов морской техники и морской инфраструктуры. Морской вестник, № 1(49), 2014, С. 113-118
4. Алексеев А.В., Смольников А.В. Интеллектуальная поддержка принятия управленческих решений при борьбе за живучесть морских объектов повышенного риска/Материалы конференции «Информационные технологии в управлении» (ИТУ-2012). -СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2012. -880 с. С. 269-275.
5. Коломойцев В.С. и др. Вероятностно-временные показатели при поэтапном применении средств защиты информации // Вестник компьютерных и информационных технологий – 2017. – № 11(161). – С.37-43. DOI: 10.14489/vkit.2017.11.pp.037-043
6. Коломойцев В.С., и др. Оценка эффективности и обоснование выбора структурной организации системы многоуровневого защищенного доступа к ресурсам внешней сети // Информатика и Космос - 2015. - № 3. - С. 69-77
7. Богатырев В.А., Богатырев С.В., Богатырев А.В. Надежность кластерных вычислительных систем с дублированными связями серверов и устройств хранения // Информационные технологии - 2013. - № 2. - С. 27-32
8. Богатырев В.А., Богатырев А.В. Функциональная надежность систем реального времени // Научно-технический вестник информационных технологий, механики и оптики - 2013. - № 4(86). - С. 150-151
9. Богатырев В. А. Отказоустойчивость и сохранение эффективности функционирования многомагистральных распределенных вычислительных систем//Информационные технологии. 1999. № 9. С. 44-48
10. Богатырев В.А., Богатырев С.В. Критерии оптимальности многоустойчивых отказоустойчивых компьютерных систем // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики - 2009. - № 5(63). - С. 92-98
11. Богатырев В.А., Богатырев С.В., Богатырев А.В. Оптимизация древовидной сети с резервированием коммутационных узлов и связей // Телекоммуникации - 2013. - № 2. - С. 42-48
12. INET Framework 4.0 User's Guide // [Электронный ресурс] – Режим доступа: https://inet.omnetpp.org/users-guide/, свободный. – Загл. с экрана.
13. GLBP - Gateway Load Balancing Protocol // [Электронный ресурс] – Режим доступа: https://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html, свободный. – Загл. с экрана.
14. GLBP (Gateway Load Balancing Protocol) // [Электронный ресурс] – Режим доступа: http://xgu.ru/wiki/GLBP, свободный. – Загл. с экрана.
15. Носков И.И. Методы и алгоритмы обеспечения надежности и отказоустойчивости компьютерных сетей // Синергия Наук - 2018. - № 24. - С. 603-616
16. Носков И.И. Протоколы обеспечения сетевой отказоустойчивости информационных экономических систем // Информационно-технологическое обеспечение цифровой экономики: сборник статей сотрудников кафедры информационных систем и технологий - 2018. - С. 66-72
17. Хабаров С.П. Моделирование Ethernet сетей в среде OMNeT++ INET framework // Научно-технический вестник информационных

технологий, механики и оптики. 2018. Т. 18. № 3. С. 462–472. doi: 10.17586/2226-1494-2018-18-3-462-472
18. Богатырев В.А., Богатырев А.В., Голубев И.Ю., Богатырев С.В. Оптимизация распределения запросов между кластерами отказоустойчивой вычислительной системы // Научно-технический вестник информационных технологий, механики и оптики - 2013. - № 3(85). - С. 77-82
19. Богатырев В.А., Богатырев С.В. Надежность мультикластерных систем с перераспределением потоков запросов//Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 2. С. 171-177
20. Богатырев В.А., Богатырев С.В. Резервированное обслуживание в кластерах с уничтожением неактуальных запросов // Вестник компьютерных и информационных технологий -2017. - № 1(151). - С. 21-28
21. Богатырев В.А., Богатырев С.В. Своевременность обслуживания в многоуровневых кластерных системах с поэтапным уничтожением просроченных запросов // Вестник компьютерных и информационных технологий - 2018. - № 2(164). - С. 28-35
22. Parshutina S.A. Models to support design of highly reliable distributed computer systems with redundant processes of data transmission and handling // 2017 International Conference «Quality Management, Transport and Information Security, Information Technologies» (IT&QM&IS), IET - 2017, pp. 96-99.

УДК 004.514.6

КВАЛИМЕТРИЧЕСКОЕ РАНЖИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА SCADA, А ТАКЖЕ ЛУЧШИХ ПРАКТИК ИХ ОСВОЕНИЯ В ЖИЗНЕННОМ ЦИКЛЕ ОБЪЕКТА МОРСКОЙ ИНФРАСТРУКТУРЫ ПО РАЗРАБОТКЕ АВТОМАТЕЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Рогозин Михаил Юрьевич
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mail: chelovekzagadka.1994@mail.ru

Аннотация. На примере анализа использования информационных технологий класса SCADA при управлении жизненным циклом объекта морской инфраструктуры по разработке автоматизированных систем управления с целью обеспечения конкурентной способности выпускаемой продукции и услуг предложено и выполнено для оптимального выбора квалиметрическое ранжирование программно-аппаратных комплексов данного класса.

Ключевые слова: класс технологии; квалиметрия; ранжирование; конкурентная способность, автоматизированная система управления техническим процессом.

QUALITATIVE RANKING OF INFORMATION TECHNOLOGY CLASS SCADA, AS WELL AS THE BEST PRACTICES OF THEIR DEVELOPMENT IN THE LIFE CYCLE OF THE OBJECT OF MARITIME INFRASTRUCTURE DEVELOPMENT AUTOMATED CONTROL SYSTEM

Rogozin Mikhail
St. Petersburg State Marine Technical University
3 Lotsmanskaya Str., St. Petersburg, 190121, Russia
e-mail: chelovekzagadka.1994@mail.ru

Abstract. On the example of the analysis of the use of information technologies of SCADA class in the management of the life cycle of the object of marine infrastructure for the development of automated control systems in order to ensure the competitive ability of products and services proposed and performed for optimal selection of qualimetric ranking of software and hardware systems of this class.

Keywords: technology class; qualimetry; ranking; competitive ability, automated control system.

Для обеспечения оптимальности выбора и использования перспективных информационных технологий (ИТ) на предприятиях морской инфраструктуры по разработке автоматизированных систем управления с целью обеспечения конкурентной способности выпускаемой продукции и услуг сегодня весьма актуальным и востребованным является обоснование предложений по оптимальному выбору, для чего, прежде всего, необходимо выполнить квалиметрическое ранжирование альтернативных программно-аппаратных комплексов реализации этих технологий.

Одной из особо востребованных ИТ следует считать технологии и системы SCADA (Supervisory Control And Data Acquisition), представляющие собой набор программных приложений, предназначенных для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга и управления.

SCADA может являться частью автоматизированной системы управления технологическими процессами (АСУТП), автоматизированной системы контроля и учёта энергоресурсов (АСКУЭ), научного эксперимента, автоматизации здания и т. д. SCADA-системы используются во всех отраслях хозяйства, где требуется обеспечивать операторский контроль за технологическими процессами в реальном времени [1].

Системы SCADA получили распространение при разработке комплексных систем автоматизации производственных процессов. Эти системы на данный момент являются основной частью передовых автоматизированных систем управления процессами. Они были широко распространены в начале прошлого столетия, сейчас уже практически на всех объектах автоматизации установлены SCADA-системы. Их широкое использование привело к значительному удешевлению эксплуатации вторичного оборудования на крупных и

средних по масштабу производственных процессов объектах путем переноса индикации и накопления информации на соответствующие пульты диспетчеризации и АРМ.

Российские SCADA-программные комплексы появились в начале 90-х годов с уже «привычным» 10-летним запаздыванием в этой области, особенно усиленным долго преодолевавшимся недоверием к надежности и технологичности этих систем. Первоначально создавались программы под конкретный объект и лишь затем появились универсальные решения. В настоящее время имеется около десятка отечественных SCADA-пакетов, причем, далеко не с равными технологическими возможностями и качеством. Именно поэтому в обеспечение конкурентной способности выпускаемой продукции предприятия заинтересованы в оптимальном выборе лучших из них для долгосрочного их использования и наращивания возможностей.

Широко распространенные как на мировом, так и на российском рынке SCADA-системы в подавляющем большинстве «ответственны» лишь за тот уровень промышленной автоматизации, который связан с получением данных от различных датчиков и устройств ввода-вывода, визуализации собранной информации и ее архивирования. Доступ же к этой информации со стороны руководства предприятия, а также руководителей экономических подразделений до недавнего времени был лишь опосредованным. Для анализа производства в целом, моделирования его отдельных этапов, выявления критических участков и слабых звеньев весьма важным является доступ к производственной информации на всех уровнях в реальном времени.

На сегодняшний момент развитие любого промышленного комплекса тесно связано с развитием SCADA-систем и их технологий. Понятно, что они будут усложняться с одновременным увеличением вычислительных мощностей и обеспечением производственной безопасности [2].

В настоящее время невозможно представить крупные промышленные предприятия, а также предприятия энергетического комплекса без оперативного диспетчерского управления и сбора данных. В ряде исследований отмечается, что в 60-х годах прошлого века ошибка операторов являлась первопричиной лишь 20 % аварий. В свою очередь, в настоящее время доля человеческого фактора прямо противоположна, то есть на долю машин выпадает лишь 20 % аварий. Аналитиками прогнозируется, что в ближайшем будущем SCADA-системы будут развиваться по тому же принципу, по которому строился их путь от первых проб до современных комплексов. Эксперты отмечают, что сложность объектов, на которых применяется подобное оборудование, количество происходящих одновременно технологических процессов и скорость изменения параметров продолжит возрастать и увеличиваться, что обусловлено требованиями к сокращению временных затрат на производство с одновременным наращиванием объемов выпускаемой продукции.

К современным SCADA – системам их пользователями (заказчиками) предъявляются, как правило, следующие основные требования:

- функциональное качество;
- надежность системы;
- безопасность использования и управления;
- точность обработки и представления данных и широкий спектр возможностей для реализации графического интерфейса;
- полнота использования новых технологических возможностей.

Исходя из требований, которые предъявляются к современным SCADA-системам, большинству современных пакетов присущи следующие основные возможности:

- Сбор и хранение первичной информации от устройств нижнего уровня;
- Обработка первичной информации;
- Управление и регистрация сигналов об аварийных ситуациях;
- Хранение информации с возможностью ее постобработки;
- Визуализация информации в виде графиков, гистограмм и т.д.

Интеллектуальная поддержка и оптимизация решений операторов по безопасному и эффективному использованию программно-аппаратных комплексов.

В этой связи ранжирование альтернативных вариантов SCADA-системам по обобщенному уровню качества для выбора заказчиками наиболее предпочтительных является весьма сложной методической и практической задачей.

Её эффективное решение сегодня невозможно без использования развитых аппаратов по измерению качества сложных организационно-технических комплексов, т.е. без совершенных технологий квалиметрического анализа.

В этом контексте нами была сформирована база данных по альтернативным вариантам ИТ класса SCADA для последующего их квалиметрического анализа по четырнадцати основным критериям: обобщённый уровень качества по данным сертификации (ОУС); функциональное качество решения задач (ФК); эргономичность (ЭС); дружественность интерфейса (ДИ); качество сервисного обслуживания (СО); длительность внедрения (ДВ); стоимость владения (СВ), включая поддержку внедрения, и др.

По результатам квалиметрического ранжирования более 15 альтернативных вариантов ИТ класса SCADA и программно-аппаратных комплексов их реализации лидирующую позицию занял программный комплекс «SCADA КРУГ – 2000», являющаяся исключительно российским продуктом.

Основными отличительными особенностями и конкурентными преимуществами программного комплекса «SCADA КРУГ – 2000» были выявлены [3]:

- надежность SCADA - системы;

– высоконадёжный отказоустойчивый протокол обмена между SCADA и системами реального времени контроллеров;

– высокая надежность передачи команд управления и обеспечения требуемого времени передачи данных в системах АСУ ТП, учёта энергоресурсов, диспетчеризации и телемеханики;

– открытость (информационная прозрачность) SCADA - системы;

– возможность технологически несложной (простой) «бесшовной» интеграции с существующими устройствами и системами;

– возможность имитационного моделирования процессов в реальном времени;

– возможность создания тренажёров для тренировок оперативного персонала на единой платформе программных и технических средств;

– гибкий выбор конфигураций модулей – от простых до сложных;

– минимизация затрат на приобретение и владение в целом SCADA - системой;

– полная импортозамещение (Российское производство) с соответствующей независимостью от иностранных производителей;

– большой выбор интерфейсных возможностей и протоколов для обмена данными и сопряжения с устройствами и программным обеспечением других производителей;

– объектно-ориентированный графический редактор и большая библиотека графических примитивов;

– возможность создания современного, гибкого, интуитивно понятного интерфейса;

– возможность точного восстановления последовательности событий на всех уровнях системы на любой момент времени и другие.

Заключение.

Концепция SCADA предопределена всем ходом развития систем управления и результатами научно-технического прогресса. Построение прикладных систем на основе любой из альтернативных SCADA-систем резко сокращает набор необходимых знаний в области традиционного программного обеспечения решаемых задач, позволяя концентрировать усилия по освоению знаний в самой прикладной области.

Применение в SCADA-системах новых технологий, разработка инструментальных средств комплексной автоматизации предприятия свидетельствуют о стремлении и возможности организаций-разработчиков постоянно совершенствовать свои продукты, что является немаловажным фактором при выборе инструментальных средств, даже если не все его технологические решения в ближайшее время будут использованы.

В этой связи постановка задачи сравнительного квалиметрического ранжирования ИТ класса SCADA, как, очевидно, и других классов ИТ, нам представляется весьма актуальной задачей, требующей привлечения широкого круга специалистов и публичного обсуждения полученных результатов. Приведенный пример квалиметрического ранжирования и обоснования оптимального выбора программного комплекса «SCADA КРУГ – 2000» подтвердил возможность, результативность и перспективность использованного подхода, методики и технологии.

СПИСОК ЛИТЕРАТУРЫ

1. Журнал «Молодой учёный», выпуск №22.5 от 2015 года. Статья Максимова Е.А., Грицюк С.Н. – «Использование SCADA-технологий в современных автоматизированных системах управления».
2. Журнал «Молодой учёный», выпуск №19 от 2018 года. Статья Афанасьева А.И. – «Основные тенденции развития SCADA-систем».
3. Сайт производителя НПФ «КРУГ». https://www.krug2000.ru/products/ppr/scada-2000.html.

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.896

ЭКОНОМИЧЕСКИЙ ПОДХОД ПРИ ОБЕСПЕЧЕНИИ СОХРАНЕНИЯ ПРАГМАТИЧЕСКОЙ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В ГРУППЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Ким Юлия Вячеславовна, Викснин Илья Игоревич
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: yulia1344@gmail.com, Wixnin@mail.ru

Аннотация. Рассмотрено взаимодействие в группе беспилотных летательных аппаратов, основанное на децентрализованной коллективной стратегии. Сделан акцент на сохранении прагматической целостности информации, и во избежание возникновения нарушений в данной категории целостности был разработан метод, основанный на теории кредита. Метод подразумевает регламентацию объема передаваемых агентами данных посредством установления фиксированного количества условных единиц информации в единицу времени (рассрочки). В случае удержания агентом данных впоследствии ценность выплат данного агента уменьшается, тем самым растет его задолженность. По окончании периода рассрочки для каждого агента вычисляется его уровень доверия и репутации. При внедрении в группу нового агента рассчитывается кредит, при котором новый агент будет получать информацию от остальных членов группы не в полном объеме, а за вычетом заданной процентной ставки. При этом он должен передавать данные в соответствии с установленными условиями рассрочки. По окончании срока кредита определяется, станет ли новый агент полноценным членом группы или будет заблокирован. Для оценки эффективности предложенного метода было смоделировано взаимодействие группы роботов, состоящей из десяти роботов. В группу внедрялось два новых агента, один из них являлся диверсантом. Пороговым значением задолженности для принятия агента в группу являлась половина от установленного размера кредита. Был реализован ряд независимых опытов, в результате которых диверсант был заблокирован в 90,8 % случаев.

Ключевые слова: децентрализованное коллективное управление; мультиагентные робототехнические системы; теория кредита; прагматическая целостность; информационная безопасность.

ECONOMIC APPROACH IN PROVIDING PRAGMATIC INFORMATION INTEGRITY PRESERVATION IN A GROUP OF UNMANNED AERIAL VEHICLES

Kim Iuliia, Viksnin Ilya
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (University ITMO)
49 Kronverksky Av., St. Petersburg, 197101, Russia
e-mails: yulia1344@gmail.com, Wixnin@mail.ru

Abstract. Interaction in a group of unmanned aerial vehicles based on decentralized collective strategy is considered. The emphasis is put on providing pragmatic information integrity, and to avoid violation occurrence in this integrity category the method based on credit theory was developed. The method implies regulation of information volume transferred by agents through establishment of fixed amount for information conventional units per time unit (installment plan). In case of data retention by agent subsequently its payment value is reduced, thus, its indebtedness is increased. In the end of installment plan period agent's level of trust and reputation is calculated. During introduction into the group of a new agent the credit is determined, due to which the new agent gets from other group members not full information but information reduced by the established interest rate. However, this agent must transmit data in accordance with predetermined installment plan conditions. In the end of credit period the decision whether the new agent is accepted or blocked is made. To assess effectiveness of the proposed method the interaction in robotic group consisted of ten agents was modelled. Two new agents were introduced into the group, and one of them was a saboteur. The threshold value of indebtedness for being accepted to the group is the half of established credit size. Series of independent tests were conducted, in the 90,8 % of them the saboteur was blocked.

Keywords: decentralized collective management; multi-agent robotic systems; credit theory; pragmatic integrity; information security.

Введение.

За последнее время мультиагентные системы получили широкое распространение в силу своей отказоустойчивости, высокой скорости взаимодействия, относительной автономности агентов. В настоящее время существует множество проектов и разработок, связанных с возможностью применения мультиагентных систем в различных сферах жизни общества. В работе [1] предлагается их использование в умных домах для оптимального распределения энергии, в статье [2] приведено проект использования мультиагентного подхода в индустрии 4.0. В данной статье мультиагентные системы рассматриваются на примере группы беспилотных летальных аппаратов (БПЛА) в контексте мониторинга открытых и закрытых участков. Под мониторингом подразумевается периодическая проверка территории на наличие нестандартных изменений. Изучаемая группа БПЛА использует коллективную децентрализованную стратегии управления: агенты имеют общий канал связи, обеспечивающий согласованность работы для решения поставленных задач.

Для корректного и эффективного функционирования группы, подчиняющейся коллективной стратегии управления, возникает необходимость обеспечения безопасности передачи информации по каналу связи. На данный момент механизмы обеспечения информационной безопасности в мультиагентных робототехнических системах подразделяют на два основных вида: механизмы обеспечения «жесткой» безопасности и механизмы обеспечения «мягкой» безопасности [3]. К первому виду данных механизмов относятся шифрование каналов связи с открытым ключом, использование мобильной криптографии, авторизация агентов. Примером механизмов «мягкой» безопасности является модель доверия и репутации к объектам [4].

Однако перечисленные выше способы ориентированы, в основном, на сохранение семантической целостности – смысловой составляющей [5,6]. Следует учитывать, что чтобы не подрывать доверие к себе ложной информацией, агенты могут достоверные факты, но не в полном объеме. В таком случае происходит нарушение прагматической целостности [7]. В данной работе большое внимание будет уделено прагматической целостности информации – категории, заключающейся в достоверности и полноте знаний, на основе которых формируется информационное сообщение.

Постановка задачи исследования. Имеется группа, состоящая из N БПЛА: $R = \{r_1, r_2, \ldots, r_N\}$. Каждый агент обладает совокупностью из M свойств: $S^i = \{r_i \mid s_j^i, j \in [1; M]\}$, $i \in [1; N]$. В качестве допущения рассматривается гомогенность роботов: $\forall r_i, r_j \in R, i \neq j, i, j \in [1; N]$: $S^i = S^j$. Предполагается, что механизмы жесткой безопасности реализованы и функционируют корректно.

Агенты взаимодействуют друг с другом в течение периода T. Данная группа функционирует на территории F, разделенной на f равных участков. БПЛА исследует каждый участок f за равные промежутки (дискреты) времени. По окончании анализа участка агенты обмениваются собранной информацией. Информация I_i, находящаяся в распоряжении каждого i-го БПЛА в конце дискреты $[t_{k-1}; t_k] \in T$ перед началом обмена с остальными членами группы делится на собственную и приобретенную. Собственная информация – это сведения о собственном техническом состоянии данного агента на текущий момент, а также сведения о техническом состоянии группы за предыдущую дискрету времени. Приобретенная информация – это данные, собранные агентом, о состоянии окружающей среды за период $[t_{k-1}; t_k] \in T$. Данные зависимости представлены в формулах (1)-(3):

$$I_{own_i} = I_{cts_{[t_{k-1};t_k]_i}} \cup \left(\bigcup_{j=1}^{N} I_{cts_{[t_{k-2};t_{k-1}]_j}}\right), \tag{1}$$

где I_{own_i} – собственная информация i-го агента, $I_{cts_{[t_{k-1};t_k]_i}}$ – информация i-го БПЛА о его собственном техническом состоянии на текущий момент, $I_{cts_{[t_{k-2};t_{k-1}]_j}}$ – информация j-го агента о собственном техническом состоянии за предыдущую дискрету времени.

$$I_{acquired_i} = I_{es_{[t_{k-1};t_k]_i}}, \tag{2}$$

где $I_{acquired_i}$ – приобретенная информация i-го агента, $I_{es_{[t_{k-1};t_k]_i}}$ – данные i-го агента о текущем состоянии окружающей среды.

$$I_i = I_{own_i} \cup I_{acquired_i} \tag{3}$$

После обмена данными каждый агент обладает информацией, как представлено в формулах (4)-(6):

$$I_{own_i} = I_{cts_{[t_{k-1};t_k]}} \cup \left(\bigcup_{j=1}^{N} I_{cts_{[t_{k-2};t_{k-1}]_j}}\right) \tag{4}$$

$$I_{acquired_i} = I_{es_{[t_{k-1};t_k]_i}} \cup \left(\bigcup_{j=1}^{N, i \neq j} \left(I_{es_{[t_{k-1};t_k]_j}} \cup I_{cts_{[t_{k-1};t_k]_j}}\right)\right) \tag{5}$$

$$I_i = I_{own_i} \cup I_{acquired_i} \tag{6}$$

Таким образом, информация, полученная путем объединения данных, переданных всеми агентами, должна стремиться к тому, чтобы полностью отражать состояние группы и окружающей среды. Это утверждение выражено формулами (7) и (8):

$$I = \bigcup_{i \in [1;N]} I_i \tag{7}$$

$$I \to U\ , \tag{8}$$

где U – полная информация о группе и окружающей среде на текущий момент.

Однако в группе могут присутствовать диверсанты, преследующие цель саботировать работу всех ее членов. Чтобы не портить свою репутацию ложными передаваемыми данными, диверсант может удерживать часть информации, при этом получая в полном объеме сведения от других агентов. Тем самым диверсант препятствует составлению полной картины о группе и окружающей среде и может замедлить продуктивность работы всей группы. Данная ситуация проиллюстрирована формулой (9):

$$\widetilde{I}_{acquired_i} < I_{acquired_d}, i \neq d\ , \tag{9}$$

где $\widetilde{I}_{acquired_i}$ – приобретенная информация i-того агента при деструктивном информационном воздействии диверсанта; d – идентификатор диверсанта в группе, $d \in [1; N]$.

Задача исследования состоит в поиске эффективных методов, позволяющих минимизировать риск деструктивного информационного воздействия на группу со стороны диверсантов и обеспечить сохранение прагматической целостности передаваемой информации: $\forall i \in [1; N]\ \widetilde{I}_{acquired_i} = I_{acquired_d} + \varepsilon$, при этом $\varepsilon \to 0$, $I \to U$.

Обеспечение прагматической целостности передаваемой информации посредством теории кредита. Для предотвращения удержания агентами информации в качестве дополнительных параметров для вычисления доверия и репутации предлагается способ, основанный на теории кредита. Под кредитом [8,9] зачастую понимают доверие, которое кредитор оказывает должнику при выдаче ссуды, что является наиболее подходящим для механизма «мягкой» безопасности. Капиталотворческая теория кредита [10,11] гласит, что кредитование способствует росту благосостояния населения. В контексте информационной безопасности кредит ведет к повышению защищенности передаваемых в группе данных.

В процессе взаимодействия группы роботов предлагается ввести понятия, а) «рассрочка», б) «кредит».

а) Время взаимодействия T делится на U периодов рассрочки заданной длины. За период рассрочки $[t_{u-1}; t_u] \in T$ каждый агент должен передать фиксированный объем информации I. В свою очередь, период взаимодействия t_u разбивается на V равных интервалов t_v^u, и по истечении каждого из них все агенты должны передать количество информации, равное I / V, как представлено в формуле (10).

$$\sum_{v=1}^{V} payment_v^u = I, U \in T\ , \tag{10}$$

где *payment* – количество информации, которое должно быть передано каждым агентом за единичный интервал периода рассрочки.

В случае если агент удержит какую-либо информацию, он нарушает фиксированный платеж, и в качестве санкции накладывается штраф, снижающий ценность выплат этого робота. Таким образом, у агента появляются задолженности. По итогам периода рассрочки будут подсчитываться задолженности каждого агента, и агенты с большим долгом будут иметь меньший показатель доверия, а, следовательно, репутации. Проверка выплат будет осуществляться в группе регулярно переизбираемым случайным образом ответственным агентом.

б) При внедрении нового агента в момент t_0 необходимо произвести его кредитование на объем переданной информации. В течение срока кредита внедренный агент должен передавать фиксированный объем информации, заданный в группе условиями рассрочки, при этом от других роботов он будет получать информацию о группе и окружающей среде с учетом вычета заданного процента. То есть в период выплаты кредита за дискрету времени $[t_{k-1}; t_k]$ после обмена информацией с другими агентами приобретенная информация j-того внедренного агента будет выражаться формулой (11):

$$I_{acquired_j} = I_{es_{[t_{k-1};t_k]_j}} \cup (1-p) \cdot \left(\bigcup_{i=1}^{N, i \neq j} \left(I_{es_{[t_{k-1};t_k]_i}} \cup I_{cts_{[t_{k-1};t_k]_i}} \right) \right) \tag{11}$$

В процессе взаимодействия процентная ставка будет уменьшаться на определенную величину, в конце полного срока кредита процентная ставка достигнет нуля. По истечении полного срока кредита проверенный агент становится полноправным членом группы, обновляет условия рассрочки, получает от других членов группы информацию в полном объеме и имеет право быть избранным ответственным агентом группы для проверки платежей. Проверка внедренных агентов:

1) сравнение заданного $payment_{must}$ и фактически полученного $payment_{got}$ по окончании срока кредита;

2) сравнение установленного $payment_{must_{u[t_{v-1};t_v]}}$ и фактического $payment_{got_{u[t_{v-1};t_v]}}$ количества информации, полученного за единичный интервал периода рассрочки, $u \in [1; U]$, $[t_{v-1}; t_v] \in [t_{u-1}; t_u]$.

3) подсчет количества несоответствий $payment_{must_{u[t_{v-1};t_v]}}$ и $payment_{got_{u[t_{v-1};t_v]}}$ в конце срока кредита.

Решение о блокировании или принятии нового агента группы принимается ответственным агентом. Предложенный способ обеспечения прагматической целостности информации снижает риск деструктивного информационного воздействия на группу. Диверсантам невыгодно внедряться в группу с высокой процентной ставкой, большим сроком кредита и коротким периодом рассрочки: большое количество проверок не дает возможности удерживать много информации, а расходы (энергетические, временные, информационные) во время кредита превышают доходы, которые могут быть получены после его погашения. Предложенный способ сохранения прагматической целостности информации был протестирован на специально запрограммированном симуляторе. Начальные условия эксперимента:

- имеется группа из 10 проверенных агентов;
- проверяемая заданной группой роботов территория состоит из 20 равных участков;
- одна условная единица времени равна времени, за которое группа проверяет один участок;
- период рассрочки равен двум условным единицам времени;
- за одну условную единицу времени каждый робот должен передать 10 условных единиц информации;
- в группу внедряют 2 новых агента: один из них является диверсантом;
- срок кредита составляет 10 условных единиц времени;
- начальная ставка процента – 50 %; по истечении каждого периода рассрочки данная ставка уменьшается на 10 %;
- предельный размер задолженности, при котором новый агент становится полноправным членом группы – половина от заданной суммы кредита;
- диверсанты в зависимости от ситуации могут передавать данные в полном объеме, либо удерживать часть информации.

Распределение размеров задолженностей диверсанта на протяжении эксперимента представлено на рис. 1:

Рис. 1. Распределение размеров задолженностей диверсанта на протяжении эксперимента

В результате проведенного эксперимента диверсанты были корректно определены, т.к. общее число опытов, в которых процент задолженности был менее 50 % составляет 9,2 %.

Заключение.

Поставленная задача исследования была выполнена. С помощью метода, основанного на теории кредита, представляется возможным минимизировать деструктивное информационное воздействие агентов-диверсантов на группу и обеспечить сохранение прагматической целостности передаваемых данных. Кредитование информации делает невыгодным саботирование работы группы, поскольку существенно замедляет процесс саботажа и требует больших затрат со стороны диверсантов.

СПИСОК ЛИТЕРАТУРЫ

1. Li W., Logenthiran T., Woo W. L., Phan V., Srinivasan D. Implementation of demand side management of a smart home using multi-agent system // 2016 IEEE Congress on Evolutionary Computation (CEC), Vancouver, BC, 2016, pp.2028-2035.
2. Wang S., Wan J., Zhang D., Li D., Zhang C. Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination // Computer Networks. №C, 2016, pp.158-168.
3. Зикратов И.А., Зикратова Т.В., Лебедев И.С., Гуртов А.В. Построение модели доверия и репутации к объектам мультиагентных робото-

технических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. №3, 2014, с. 30-38.
4. Бешта А.А., Кирпо М.А. Построение модели доверия к объектам автоматизированной информационной системы для предотвращения деструктивных воздействий на систему // Известия Томского политехнического университета. № 5, 2013, с. 104-108.
5. Jovanov I., Pajic M. Sporadic data integrity for secure state estimation // 2017 IEEE 56th Annual Conference on Decision and Control (CDC), 2017, pp. 163-169.
6. Santra P., Roy A., Majumder K. A Comparative Analysis of Cloud Forensic Techniques in IaaS // Advances in Computer and Computational Sciences / Advances in Intelligent Systems and Computing. №554, 2017, pp.207-215.
7. Комаров И.И., Дранник А.Л., Юрьева Р.А. Моделирование проблем информационной безопасности мультиагентных систем // В мире научных открытий. № 4, 2014, с. 61-70.
8. Лаврушин О.И. Базовые основы теории кредита и его использование в современной экономике // Вопросы регулирования экономики. №2, 2017, с.6-15.
9. Евтух А.Т. Теория кредита: социально-экономический аспект // Финансы и кредит. №25, 2005, с. 21-27.
10. Гурнакова Л.Н. Сущность, теоретические основы понятия «Кредитный рынок» // Проблемы современной экономики. №2, 2011, с. 83-85.
11. Костерина Т.М., Панова Т.А. Методологические основы анализа границ кредита // Финансы и кредит. №32, 2015, с. 26-38.

УДК 004.056.5

РАЗРАБОТКА МЕТОДА ОБНАРУЖЕНИЯ И КОРРЕКЦИИ ОШИБОК ДЛЯ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СЕТИ НА ОСНОВЕ БОЛЬШИХ ДАННЫХ

Леснова Елена Михайловна, Пестов Игорь Евгеньевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: lesnova.e.m@gmail.com, pestovie@outlook.com

Аннотация. Рассматривается проблема необходимости реализации системы сетевого контроля в распределенной информационной сети с использованием Больших данных. Для обеспечения обнаружения вторжений предлагается использовать улучшенную мультиагентную систему на основе GRID-вычислений.

Ключевые слова: GRID-вычисления; Большие данные; программные агенты, обнаружение вторжений, распределенные информационные сети.

DEVELOPMENT OF THE METHOD OF DETECTION AND CORRECTION ERRORS FOR BIG DATA BASED DISTRIBUTED INFORMATION NETWORK

Lesnova Elena, Pestov Igor
Bonch-Bruevich Saint-Petersburg state university of communication
22/1 Bolshevikov Av., St. Petersburg, 193232, Russia
e-mails: lesnova.e.m@gmail.com, pestovie@outlook.com

Abstract. It is considered a problem of the need to implement a network control system in big data based distributed information network. For intrusion detection guaranteeing it is proposed to use a based GRID-computing improved multi-agent system.

Keywords: GRID-computing; Big data; software agent; intrusion detection; distributed information network.

Построение распределенных информационных сетей (РИС), устойчивых к компьютерным атакам, сопряжено со значительными затратами времени и материальных ресурсов. Обеспечение работоспособности РИС и функционирующих в ней дополнительных систем часто зависит от способности РИС противостоять целенаправленным воздействиям, нарушающим её работу. Для РИС основной проблемой является низкая эффективность обнаружения неизвестных атак и защиты от внутреннего нарушителя.

Современные РИС характеризуются сверхвысокими объемами интенсивно поступающего разнородного сетевого трафика, в связи с чем актуально рассмотрение систем обнаружения вторжений (СОВ), направленных на обработку Больших данных. Однако, математические аспекты построения СОВ и мониторинга РИС для определения внутреннего нарушителя на сегодняшний день разработаны еще недостаточно, а механизмы скрытого мониторинга и работы Больших данных существуют по отдельности. Поэтому именно построение перспективных распределенных систем обнаружения вторжений (РСОВ) с использованием методов скрытого мониторинга и анализа Больших данных является актуальным.

В качестве известного примера, на основе агентного подхода можно построить структуру GRID-сети. Описанное в работе использование технологии GRID позволит РСОВ использовать параметры ПК для поиска решений сбора данных [1]. При намерении совершить атаку злоумышленник сможет подать команду, например, winlog – вирус, который рекомендуется уничтожить или переместить в карантин. Вероятно, часть участников системы успеют выполнить рекомендации до того, как РСОВ сможет предотвратить сбой. Исследования и разработки в сообществе GRID имеют особенности протоколов и сервисов, направленных и на проблемы, которые возникают при попытке создания масштабируемых ИС [2-4].

В статье предлагается внедрение методики обнаружения вторжений, исследованное ранее в работах [2-5]. Необходимость данной методики обусловлена не только широким применением РСОВ в РИС, но и важностью использования временных рядов для снижения временных затрат на обнаружение вторжений. Первоначально имеется в виду входящий трафик РИС для контроля действий внешнего нарушителя [6].

Предполагается [1,5,6], что на первом этапе методики исходный трафик будет разбит на временные окна, которые не должны пересекаться между собой. В каждом из окон будут формироваться временные ряды и извлекаться ключевые параметры выбранного протокола. По итогам вышеперечисленных действий будут получены данные, соответствующие виду:

$$\text{Окно}_i = \begin{cases} \text{Временной ряд для параметра}_1 \\ \text{Временной ряд для параметра}_2 \\ \text{Временной ряд для параметра}_3 \end{cases} \quad (1)$$

Следующим действием на вход дискретного вейвлет-преобразователя будут поданы все полученные последовательности, в результате чего будут получены необходимые для анализа коэффициенты детализации. Также требуется охарактеризовать поведение сетевого трафика во временных окнах, для чего целесообразно отслеживать степень зависимости различных параметров сетевого пакета. Для этого был введен коэффициент множественной корреляции, вычисляемый для последовательностей x, y, z следующим образом:

$$R_{y(x,z)} = \sqrt{\frac{r_{xy}^2 + r_{zy}^2 - 2 * r_{xy} * r_{zy} * r_{xz}}{1 - r_{xz}^2}}; \quad (2)$$

где r_{xy}, r_{zy}, r_{xz} – парные коэффициенты корреляции, вычисляемые по формуле:

$$r_{xy} = \frac{\sum(x_i - <x>) * (y_i - <y>)}{\sqrt{\sum(x_i - <x>)^2 * \sum(y_i - <y>)^2}} \quad (3)$$

На наличие аномалии в сетевом трафике будет указывать значимое отклонение коэффициента множественной корреляции $R_{y(x,z)}$ от нормального значения. Разрабатывая РСОВ, необходимо сравнивать все модули и компоненты, которые синтезируются в единую архитектуру в процессе анализа временных рядов. На рис. 1 изображена схема работы методики обнаружения вторжений с дополнительным использованием краткосрочного прогнозирования.

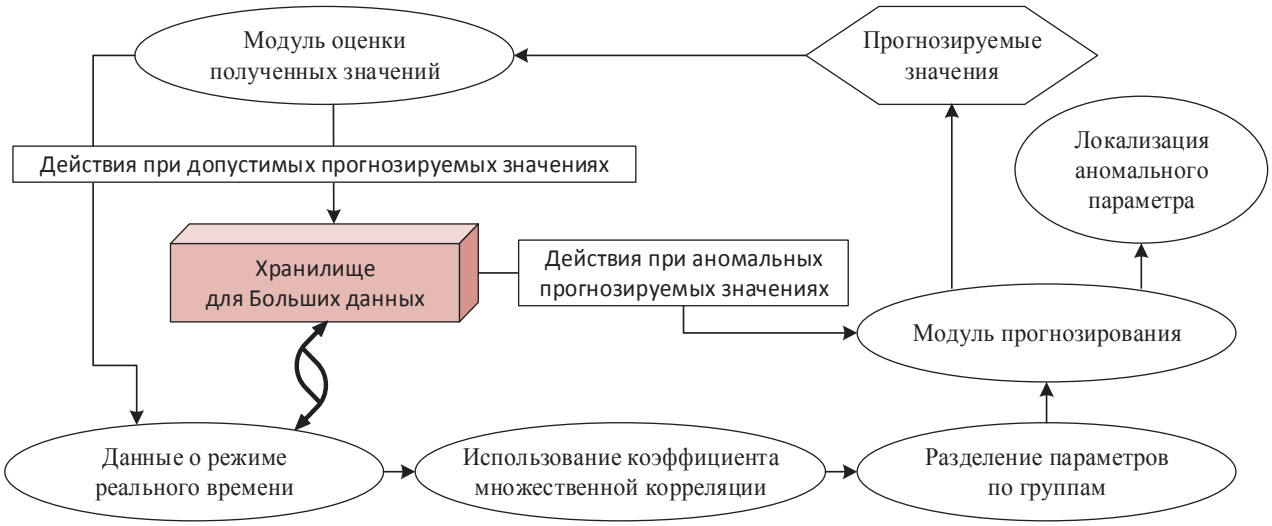


Рис. 1. Схема работы методики обнаружения вторжений с дополнительным использованием краткосрочного прогнозирования

Объем передаваемого сообщения влияет на количество времени T_1, требуемое для выявления фрагментированных пакетов в процессе обнаружения компьютерной атаки. На основании результатов анализа всех пакетов, поочередно принятых за время T_2, определяется наличие компьютерной атаки, которая начинает выявляться без ожидания дефрагментации всего сообщения.

Вышеперечисленные процессы описывают способ-прототип и служат подтверждением эффективности методики обнаружения вторжений. На рис. 2 представлен пример алгоритма шаблона атаки, задаваемый выявленными параметрами.

Связи между шаблонами атак формируются на основе пред- и постусловий, которые определяются на основе уязвимостей атакуемого хоста и уязвимостей, соответствующих текущему шаблону атаки [4].

Разница в требуемом времени для обнаружения компьютерной атаки $\Delta T = T_1 - T_2$. Если фрагментированное сообщение достаточно объемно, то достигается сформулированный технический результат при реализации заявленного способа, т.е. повышение оперативности обнаружения компьютерной атаки на РИС.

Для РИС с использованием Больших данных [7-9] принципиально важен первичный структурный анализ для повышения эффективности обнаружения выбранных шаблонов атаки по представленной методике [1,5]. За основу построения методики берутся предложенные ранее [2-5] четыре категории обработки Больших данных в процессе работы РСОВ.

Первая категория предполагает содержание в Больших данных определенной информации о вторжениях. Вторая категории содержит полиморфные алгоритмы, запутывающие противника. Наличие вторжений и

найденных объектов выявляется в третьей категории, а в четвертой при отсутствии обнаруженных угроз определяются неудачные действия РСОВ.

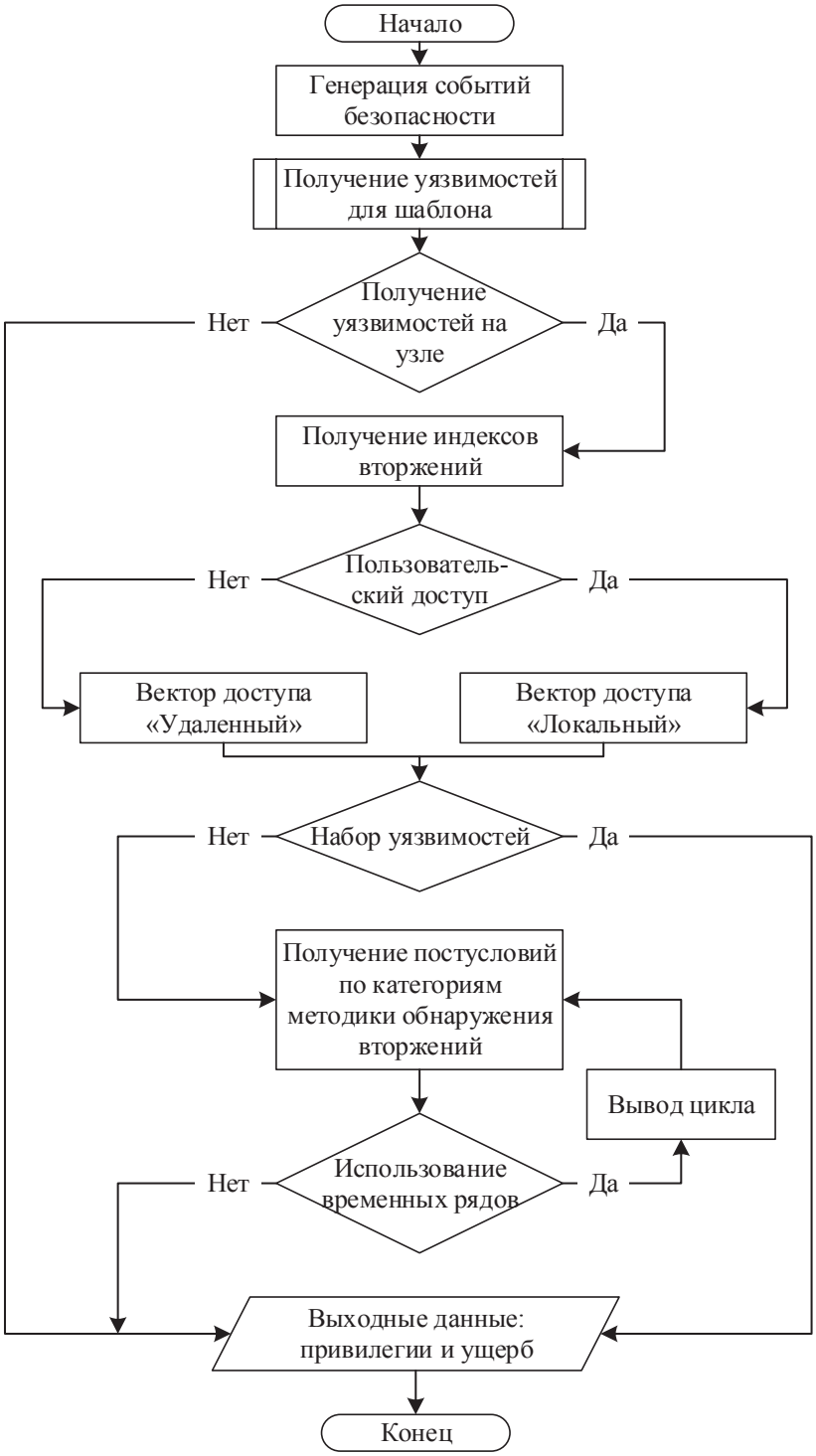


Рис. 2. Алгоритм выбора шаблона атаки для анализа в РСОВ

Обобщенная структура РИС с использованием Больших данных на основе методики обнаружения вторжений может быть представлена с помощью формулы:

$$N = S(t) + I(t) + R(t) + D(t) \quad (4)$$

где N – общее количество объектов в системе (общий диапазон до 1600 объектов во всех тестах); $S(t)$ – количество объектов без действий; $I(t)$ – количество объектов с действием (t – Примерное время выполнения до 200 сек), $R(t)$ – количество объектов с действием корреляционного анализа, $D(t)$ – количество объектов, в которых обнаружены вторжения, запущенные с помощью РСОВ.

Полученные зависимости изменения количества пораженных узлов от времени функционирования РИС [7] в условиях распространения вторжения представлены на рис. 3 (горизонтальная шкала – количество объектов в системе, вертикальная – время обнаружения вторжений в сек.).

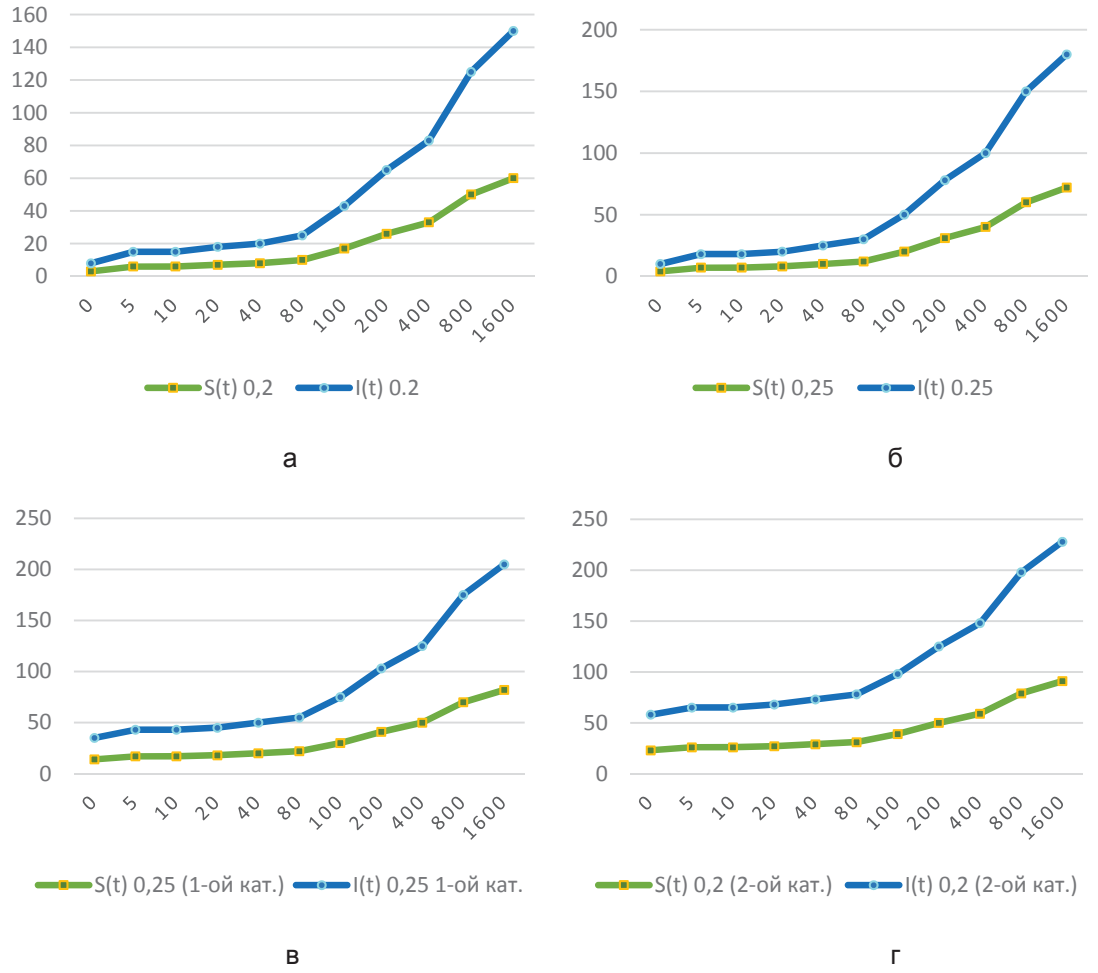


Рис. 3. Зависимости изменения количества узлов от времени функционирования *а* – $\beta = 0{,}2$; *б* – $\beta = 0{,}25$ и $k = 0{,}02$; *в* – первый этап сбора данных, β=0,25, $k = 0{,}02$, *г* – второй этап сбора данных, при β=0,25, $k = 0{,}02$

В общем итоге по графику на рис. 4 получается, что по совершенным операциям распространение ошибок в предлагаемой РСОВ [1] значительно возрастает к обработке по категориям 2 и 3, однако их уровень не так критичен. Данные результаты расчетов объясняются лишь тем, что чем больше действий приводят к обнаружению вторжений, тем больше увеличиваются риски ИБ для ПО [5]. Во всех проведенных тестах демонстрируется вероятность успеха различного рода атак, которая практически никогда не доходила до 100%, в то время как вероятность по необнаружению многих действий нарушителя были всегда от 50%.

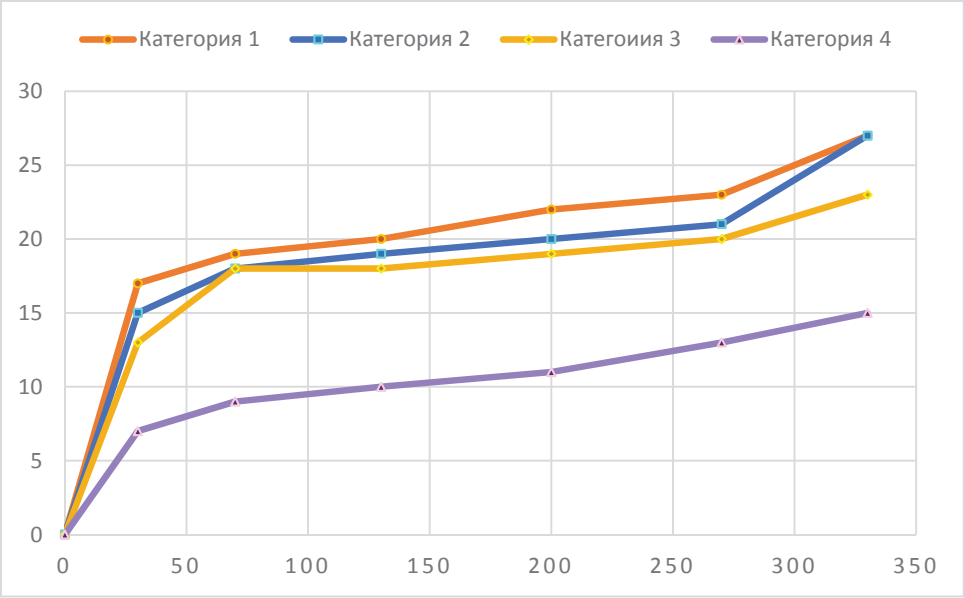


Рис. 4. Оценка вероятности обнаружения вторжений РСОВ в ходе различных атак (оранжевым цветом – для категории 1, синим – для категории 2, желтым – для категории 3, лиловым – для категории 4)

Итого следует, что предложенная методика обнаружения вторжений с использованием Больших данных в качестве среды РИС повышает эффективность выявления различного рода атак при помощи временных рядов. Была осуществлена совокупность мер с использованием полученных данных и информации, расширенной благодаря применению иерархического набора показателей, которые, в свою очередь, основываются на анализе временных рядов. За счет постоянного отслеживания и пересчета показателей пользователей данный способ позволяет снизить уровень возможных потерь от компьютерных атак. Дополнительно представлены критерии и результаты сравнительной оценки существующих способов и подходов к построению ПО РСОВ.

СПИСОК ЛИТЕРАТУРЫ

1. Герлинг, Е. Ю. Модели нарушителей информационной безопасности / Е. Ю. Герлинг, Е. И. Кулишкина, Э. В. Бирих, Л. А. Виткова// Известия высших учебных заведений. Технология легкой промышленности. — 2017. — Т. 35. — № 1. — С. 27-30.
2. Штеренберг, С. И. Методы использования пустых секций исполнимого файла для стеговложения саморазвивающегося кода в распределенной системе однозначного отождествления / С. И. Штеренберг, Л. А. Виткова, В. И. Андрианов // Системы управления и информационные технологии. — 2015. — Т. 59. — № 1-1. — С. 189-194.
3. Штеренберг, С. И. Методика применения концепции адаптивной саморазвивающейся системы / С. И. Штеренберг, Л. А. Виткова, В. П. Просихин// Информационные технологии и телекоммуникации. — 2014. — Т. 2. — № 4. — С. 126-133.
4. Шариков, П. И. Исследование уязвимости сериализации и десериализации данных в java/ П. И. Шариков, А. В. Красов// Региональная информатика и информационная безопасность: сб. науч. тр. — Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. — 2017. — С. 333-336.
5. Штеренберг, С. И. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя / С. И. Штеренберг, М. А. Полтавцева// Проблемы информационной безопасности. Компьютерные системы. — 2018. — № 2. — С. 59-68.
6. Душин, С. Е. Численное моделирование систем управления: учеб. пособие для студентов вузов, обучающихся по направлениям 550200, 651900 «Автоматизация и упр.» подгот. бакалавров, магистров и дипломир. специалистов / С. Е. Душин, А. В. Красов, Н. Н. Кузьмин, Л. Б. Пошехонов — М-во образования РФ. С.-Петерб. гос. электротехн. ун-т «ЛЭТИ»; [С. Е. Душин и др.]. СПб., 2003.
7. Дубровин, Н. Д. Реализация прототипа на базе hadoop для анализа больших данных / Н. Д. Дубровин, И. А. Ушаков, И. В. Котенко // Информационная безопасность регионов России (ИБРР-2015) Материалы конференции. — 2015. — С. 69-70.
8. Ушаков, И.А. Анализ методик применения концепции больших данных для мониторинга безопасности компьютерных сетей/ И. А. Ушаков, И. В. Котенко, К. Ю. Крылов // Информационная безопасность регионов России (ИБРР-2015) Материалы конференции. — 2015. — С. 75-76.
9. Дешевых, Е.А. Интеграция SIEM-систем с системами корреляции событий безопасности, основанных на технологии больших данных / Е. А. Дешевых, И. А. Ушаков, А. А. Чечулин // Информационные технологии в управлении (ИТУ-2016) Материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В. Г. Пешехонов. — 2016. — С. 684-687.

УДК 004.942

МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ ГРУППЫ БЕСПИЛОТНЫХ ЛЕТАЮЩИХ АППАРАТОВ В СРЕДЕ СИМУЛЯЦИИ V-REP

Турсуков Никита Олегович, Мариненков Егор Денисович
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: stepingnik@gmail.com, mandarin-98@mail.ru

Аннотация. В работе реализовывается функционирования группы беспилотных летающих аппаратов, тестируется поведение аппаратов при деструктивном воздействии на работу.

Ключевые слова: беспилотные летающие аппараты; симуляция поведения роботов.

MODEL OF FUNCTIONING OF THE PILOTLESS FLYING DEVICES IN THE ROBOT SIMULATION ENVIRONMENT V-REP

Tursukov Nikita, Marinenkov Egor
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (University ITMO)
49 Kronverksky Av., St. Petersburg, 197101, Russia
e-mails: stepingnik@gmail.com, mandarin-98@mail.ru

Abstract. In work is implemented functioning of group of the pilotless flying devices, and tested the behavior of devices at destructive impact on work.

Keywords: pilotless flying devices; simulation of robot behavior.

При разработке сложных систем с участием роботов, необходимо подробно описывать не только математическую модель ее работы, но, в том числе, предсказывать поведение роботов (агентов). Это также подразумевает предсказывание поведения в непредсказуемых ситуациях, таких как намеренные или непреднамеренные деструктивные воздействия на аппараты [1]. В таких случаях тестирование функционирования системы производится в симуляторах, позволяющих как проконтролировать поведение роботов, так и провести эксперименты с целью протестировать чрезвычайные ситуации. В представленной работе реализована модель функционирования группы беспилотных летающих аппаратов (БПЛА) с помощью фреймворка для симуляции роботизированных систем V-REP (Virtual robot experimentation platform).

Эксперименты, проведенные с помощью модели, ставят задачу ввести деструктивную информацию в процесс информационного взаимодействия БПЛА, приводящую к нарушению функционирования агента или группы в целом. Это позволило выявить необходимость в повышении уровня защиты аппаратов от деструктивного информационного взаимодействия.

V-REP представляет собой среду для построения и симуляции моделей поведения роботов, без необходимости физического доступа к аппарату [2]. Фреймворк позволяет использовать как встроенные плагины, так и писать собственные скрипты для реализации поведения роботов. Визуализация действий аппаратов реализована в трехмерном пространстве, позволяющем наглядно показать их взаимодействия.

Эксперименты функционирования БПЛА реализовывались с помощью встраиваемых скриптов, позволяющих программировать управление и поведение роботов напрямую в симуляторе, без установки дополнительного ПО. Используется встроенный редактор, поддерживающий скриптовый язык программирования Lua.

Основные характеристики частного случаю функционирования системы (эксперимента):

- квадратная область (далее – Помещение), по которой перемещаются агенты;
- 5 агентов;
- 10 флагов - 10 задач;
- область А – область старта/ область сдачи задания;
- потрачено минимум времени на выполнение задачи;
- выполнены все задачи;
- агенты – материальные точки.

Квадратная область, по которой перемещаются агенты, разделяется на 100 квадратов (площадь 10x10). Область А занимает 5 квадратов, по одному БПЛА на клетку. Точка сдачи задания у агента – того же стартовый квадрат в области А. Каждый робот имеет достаточный запас энергии, для выполнения задачи. Флаг может стоять в любом квадрате в помещении (не включая область А).

Ход работы системы:

- Группа агентов начинает функционировать в области А на территории Помещения. Целью группы является выполнение всех задач. Задачей является перемещение флага в область старта (А), т.е. перемещение к точке, где находиться флаг, и дальнейшее перемещение в область А. Окончанием эксперимента является достижение цели.
- Этапы, которые необходимо выполнить для реализации эксперимента:
- создание группы агентов;
- введение алгоритма распределения задач между агентами;
- реализация выполнения задач агентами;
- организация деструктивного воздействия на реализованную модель;
- сбор полученных данных о времени на реализацию и эффективности выполнения задач и их последующее сравнение.

Агенты общаются между собой во время движения, тем самым распределяя между собой задачи. Выбор определенной задачи робот обосновывает расстоянием между ним и флагом в Помещении (выбор ближайшего флага). Если задачу не выбрал другой агент, робот начинает ее выполнение, в то же время, сообщая об этом остальным агентам.

Деструктивное воздействие на модель реализовано в виде шестого агента-диверсанта, участвующего в распределении задач между агентами, но не реализующего выполнения полученных задач.

Описание реализации взаимодействия БПЛА в модели:

Моделью БПЛА является Quadricopter из стандартной библиотеки роботов V-REP.

Задачи представляют собой массив координат targets. Каждый элемент массива представляет собой координаты по осям и X и Y. Каждый аппарат хранит в памяти координаты задач, а также свои собственные стартовые координаты в трехмерном пространстве, сохраненные в виде coordinates.

В начале функционирования системы, агенты поднимаются на определенную высоту по оси Z, которая не меняется на протяжении полета. Агент определяет расстояние до каждого из десяти флагов, на основе своей точки старта и известных координат. После расчета расстояний до флагов, результаты сохраняются в массив results. Элементы данного массива соотносятся с массивом targets, таким образом, выбирается индекс данного массива (ближайшие координаты).

Робот начинает принимать сигналы от других агентов из группы. Если получает информацию о том, что выбранные координаты заняты, то берет следующие ближайшие к нему координаты флага и повторяет цикл до тех пор, пока не найдет не занятую задачу. При нахождении не выбранного флага, агент отправляет индекс массива targets другим роботам, таким образом, сигнализируя о том, что задача занята.

Движение агента к флагу реализовано через следование модели за привязанной к ней точкой. К точке применяется функция движения, в которой значение скорости по координатам осей X и Y зависит от расположения флага, к которому летит робот. Каждую секунду робот сравнивает свои текущие координаты с координатами флага, и если произошел сбой в маршруте, изменяет скорость движения по нужной оси. После достижения агентом области видимости флага (2 клетки), выполняется приземление на координаты с флагом, при этом меняя значение по оси Z на 0 (приземление).

После взятия флага, робот аналогичным образом движется в область А, где приземляется на точку своего старта. После этого происходит сбор данных об израсходованной энергии – от первоначального заданного количества вычитается энергия, потраченная на выполнение задачи. Информация о потраченной энергии, а также информация о выполнении задачи записываются в файл.

С помощью встроенных инструментов для графического отображения данных на плоскости, робот отмечает на поле выполненную цель. После этого повторяет действия, начиная от выбора ближайшего флага. В случае, если все задачи выполнены или уже выполняются, агент остается на поле.При задействовании в модели шестого агента-диверсанта, собираются те же данные о потраченной энергии роботов и выполненных целях.

Таким образом, после реализации модели функционирования БПЛА можно сравнить потери при деструктивном воздействии на работу системы, оценить поведение роботов в их обычном режиме работы и в критических ситуациях.

СПИСОК ЛИТЕРАТУРЫ

1. Мордвинов Дмитрий Александрович, Литвинов Юрий Викторович Обзор применения формальных методов в робототехнике // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. 2016. №1 (236).
2. С.В. Сорокин, И.В. Сорокина, И.С. Солдатенко Использование виртуальных лабораторий в инженерном образовании // Инженерное образование, 2017.

УДК 004.052.2

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦИФРОВОГО ПРОИЗВОДСТВА

Усова Мария Андреевна
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: gipurer@gmail.com

Аннотация. Были рассмотрены основные аспекты информационной безопасности цифрового производства. Была смоделирована система цифрового предприятия и информационного пространства данной системы. Определены и классифицированы основные угрозы информационной безопасности цифрового производства.

Ключевые слова: информационная безопасность; информационное пространство; цифровое производство; угрозы информационной безопасности.

INFORMATION SECURITY THREATS OF DIGITAL MANUFACTURING

Usova Maria
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (University ITMO)
49 Kronverksky Av., St. Petersburg, 197101, Russia
e-mail: gipurer@gmail.com

Abstract. The main aspects of digital production information security were considered. The system of digital manufacturing and information space of this system were modeled. The main threats to the information security of digital manufacturing were identified and classified.

Keywords: information security; information space; digital manufacturing; information security threats.

Введение.

К концу XX века в производственной сфере использовались различные подходы к созданию автоматизированных производств, снижающих долю участия человека в технологическом производстве товаров и услуг [1]. С возрастанием потребностей общества возникла необходимость в пересмотре подходов к организации производства и переходу к высокотехнологичным, “умным”, цифровым производствам, являющимся полностью автономными. Концепцию таких производств называют Индустрией 4.0. Основу ее составляют сенсоры, осуществляющие сбор информации, сеть Интернет в целом и облачные сервисы в частном. Концепция Индустрии 4.0 воплощается в военной, промышленной, бытовой сферах. Цифровое производство – информационная модель высокотехнологичного производства, процесса создания какого-либо продукта внутри цифровизированного предприятия [2,3]. Смежным цифровому производству является понятие цифровой экономики, т.е. экономической деятельности, основанной на цифровых технологиях. Она включает в себя программно-аппаратные средства и электронный бизнес. Методы цифровой экономики используются на заключительных стадиях цифрового производства при организации продажи товаров и услуг в сети Интернет. Сейчас актуальным становится вопрос обеспечения информационной безопасности данной концепции [4,5,6].

Классическая задача обеспечения ИБ направлена в первую очередь на решение задачи корректной передачи информационного сообщения. Иными словами, в первую очередь рассматривается вопрос обеспечения синтаксической целостности сообщения. В контексте кибер-физических систем особую важность приобретают

синтаксические и семантические свойства информации. Следовательно, понятие информационной безопасности расширяется, т.к. возникает необходимость в использовании дополнительных мер защиты информации.

Процесс разработки комплекса мер, направленных на защиту информации в системе цифрового производства, включает в себя этапы, изображенные на рис.1, которые позволят актуализировать проблему ИБ на стадии производства в Индустрии 4.0, а также рассмотреть аспекты ИБ для последующей организации защиты системы и определить слабо защищенные части системы.

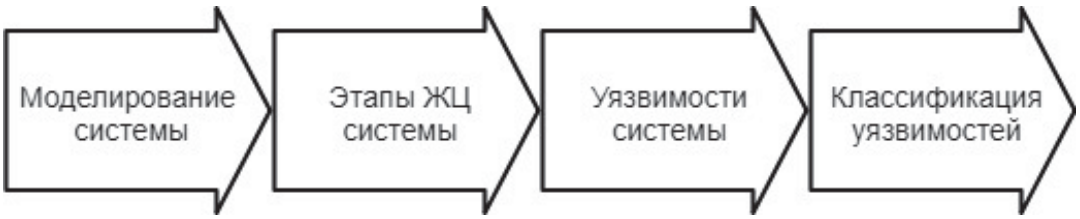


Рис. 1. Этапы разработки комплекса мер обеспечения ИБ

Моделирование системы. Модель системы позволяет визуализировать процессы, протекающие при взаимодействии объектов системы цифрового предприятия на абстрактном уровне. При создании модели системы будем пользоваться понятиями теории множеств. Представим исследуемый объект – абстрактное цифровое предприятие – как совокупность математических объектов в виде структуры $< A, I, R, Pr >$. Элементами структуры будем принимать множества объектов данной системы – множество агентов-роботов, информационное пространство, множество ресурсов, множество изделий (продуктов цифрового производства).

Множество роботов-агентов (далее - агенты) $A = \{(a_1|q_1), (a_2|q_2), \dots, (a_n|q_1)\}$ реализует сборку изделия. q_i- значение, характеризующий уровень доступа агента к элементарным сообщениям информационного пространства, $0 \le q_i \le 1$.

Каждый i-ый агент выполняет множество функций-команд $F_i = \{f_1, f_2, \dots, f_m\}$, агенты множества коммуницируют с помощью информационного пространства I.

Информационное пространство, представленное на рис. 2, – это структура $< I, D >$: $I = \{i_1, i_2, \dots, i_l\}$ – множество элементарных информационных сообщений,

$D = \{d_1, d_2, \dots, d_l\}$, $0 \le d_i \le 1$ – множество элементов, характеризующих параметры доступа к i-му информационному сообщению. Агент a_i получает доступ к сообщению i_k, если выполняется условие $q_i \ge d_i$.

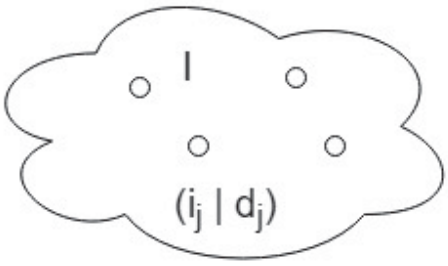


Рис.2. Информационное пространство

Множество ресурсов, используемых в производстве обозначим $R = \{r_1, r_2, \dots, r_s\}$. Множество произведенных изделий обозначим $Pr = \{pr_1, pr_2, \dots, pr_v\}$. с другой стороны $pr_i = f(A_i, R_i, I, t)$, где t – время. Если Q – пространство цифрового производства. $A, R, < I, D > \in Q$, тогда: $Q \to Pr$.

Информационное пространство включает в себя подмножество элементарных сообщений-команд, цепочек-алгоритмов для реализации сборки изделия и запросов клиента, что может быть также представлено в виде отдельных кластеров информации:

$$I = I_{function} \cup I_{rules} \cup \dots \cup I_{client} \quad (1)$$

Информационное пространство также может быть изображено в двумерном пространстве ID (рис. 3а) и в трехмерном (рис. 3б). В двумерном пространстве координатные оси – множество элементарных сообщений и соответствующие им значения параметра доступа, определяемых для k-го стороннего агента. В трехмерном пространстве ось a – ось агентов-отправителей сообщений, b – ось агентов-получателей, t – момент времени, в который сообщение было передано, при этом введем допущение, что время передачи сообщения стремится к нулю ($t_{transmisson} \to 0$). Переданное сообщение i_{ab} обладает следующими свойствами:

Агент-отправитель, a имеет безграничный доступ к данному сообщению;

Показатель уровня доступа d сообщения i_a для стороннего k-го получателя $i_a = i_{ab} \cup i_{abc}$. Данный параметр может быть спроецирован в двумерную систему координат, изображенную на рис. 3а.

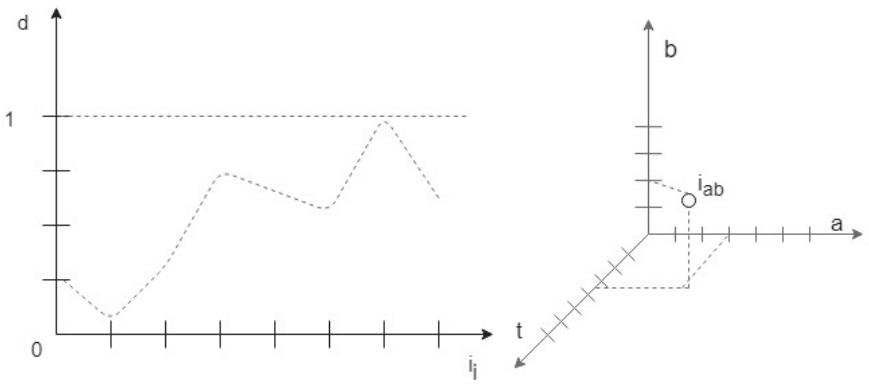


Рис. 3а, б. Информационное пространство в двумерном, трехмерном представлении

В контексте такого информационного пространства меняются понятия конфиденциальности, целостности и доступности. Конфиденциальность может быть обеспечена с помощью разграничения прав доступа к элементарным сообщениям ИП, что управляется с помощью параметров доступа d, p. Целостность информации обеспечивается путем прямого взаимодействия получателя и отправителя по схеме $A - B$, без промежуточных звеньев в цепи. Доступность, возможность обращения к сообщению i_j, отправленного агентом a агенту b, обусловлена следующим свойством информационного пространства: при проекции сообщения i_j на координатные плоскости tOa, tOb можно определить момент времени t_j, в которое оно было отправлено и определить его положение в информационном пространстве по данному идентификатору. Уязвимости системы. Этапы жизненного цикла системы. Классификация уязвимостей.

Для оценки уязвимостей системы проанализируем жизненный цикл системы. Жизненным циклом цифрового производства будем считать период времени с момента возникновения потребности в цифровизации производства до морального устаревания концепции цифрового производства. При этом введем допущение, что система не масштабируема, следовательно, количество роботов на производстве постоянно, внедрение нового робота допускается только в случае невозможности устранения поломки, потому диверсия в данной системе исключается. Выделим следующие этапы жизненные цикла системы:

– конструкторская разработка изделия: на данном этапе цифрового производства происходит работа с информацией об изделии (сведения о конструкции, технологии производства, качество продукта и др.), такие данные являются конфиденциальными. Нарушение сотрудниками компании условий коммерческой тайны приведет к снижению конкурентоспособности компании, разглашению данных о потребителях продукции, снижение уровня уникальности технологии. Нарушители используют уязвимости роботов, их комплектующих и уязвимости облачных хранилищ для получения необходимых данных;

– подготовка и настройка оборудования, подключение к сети Интернет: злоумышленник-диверсант в лице ответственного за подключение оборудования к сети Интернет может установить подключение к сторонним серверам и осуществлять передачу информации третьей стороне;

– процесс производства изделия/предоставление услуги пользователю: процесс взаимодействия объектов системы цифрового производства осуществляется по каналам связи через сеть Интернет. Уязвимости каналов связи, уязвимости ПО, контроллеров увеличивают шансы на осуществление неавторизованного доступа к объектам системы и получению информации по уязвимым каналам связи, возможно действие вредоносных программ на операционные системы роботов;

– продажа итогового изделия, утилизация остаточных данных о продукте: уязвимости, связанные с неполным удалением остаточной информации о продукте, потребителе, покупателе.

Заключение.

Анализ существующих уязвимостей ИБ является основой для создания моделей угроз и нарушителей, проведения анализа рисков и последующей разработки комплекса мер, направленных на повышение защищенности информации в цифровом производстве. При распространении концепций цифрового производства и Индустрии 4.0 возникает потребность в том, чтобы сделать их применение безопасным как для компаний, так и для потребителей услуг и продукции, в том числе обеспечить безопасность используемых данных на различных стадиях производства.

СПИСОК ЛИТЕРАТУРЫ

1. Григорьев С. Н., Кутин А. А., Долгов В. А. Принципы построения цифровых производств в машиностроении // Вестник МГТУ Станкин. – 2014. – №. 4. – С. 10-15.
2. Селиванов С.Г., Гузаиров М.Б., Кутин А.А. Инноватика. – М.: Машиностроение, 2013. – 640 с.
3. Баекер М. Цифровые технологии улучшают принципы бережливого производства // САПР и графика. – 2012. – №. 7. – С. 42-43.
4. Андиева Е. Ю., Фильчакова В. Д. Цифровая экономика будущего, индустрия 4.0 // Прикладная математика и фундаментальная информатика. – 2016. – №. 3. – С. 214-218.
5. Zhang Z. K. et al. IoT security: ongoing challenges and research opportunities // Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. – IEEE, 2014. – С.230-234.
6. Suo H. et al. Security in the internet of things: a review //Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on. – IEEE, 2012. – Т. 3. – С.648-651.

УДК 004.056

МОДЕЛЬ ПОЛИЦЕЙСКИХ УЧАСТКОВ С ЧАСТИЧНО ЦЕНТРАЛИЗОВАННЫМ УПРАВЛЕНИЕМ В МОБИЛЬНОЙ РОБОТОТЕХНИЧЕСКОЙ СИСТЕМЕ

Чупров Сергей Сергеевич, Викснин Илья Игоревич, Усова Мария Андреевна
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: drmyscull@gmail.com, wixnin@cit.ifmo.ru, gipurer@gmail.com

Аннотация. В работе произведен анализ нескольких механизмов обеспечения безопасности в мобильных робототехнических системах. Авторами был сделан вывод об отсутствии универсального подхода к обеспечению информационной безопасности и была описана разработанная схема функционирования, основанная на модели полицейских участков. Использование разработанной схемы функционирования позволяет обеспечить целостность и доступность информации, передаваемой между агентами системы.

Ключевые слова: модель полицейских участков; мультиагентная робототехническая система; мобильная робототехническая система; информационная безопасность; агент.

POLICE OFFICE MODEL WITH PARTIALLY CENTRALIZED CONTROL IN MOBILE ROBOTIC SYSTEM

Chuprov Sergey, Viksnin Ilia, Usova-Maria
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (University ITMO)
49 Kronverksky Av., St. Petersburg, 197101, Russia
e-mails: drmyscull@gmail.com, wixnin@cit.ifmo.ru, gipurer@gmail.com

Abstract. The paper analyzes several security mechanisms in mobile robotic systems. The authors concluded that there is no universal approach to ensuring information security and described the developed scheme of functioning, based on the model of police offices. The use of the developed scheme of functioning allows to ensure the integrity and availability of information transmitted between system agents.

Keywords: police office model; multiagent robotic system; mobile robotic system; information security; agent.

Введение.

Бурное развитие эры робототехники началось в 60-е годы прошлого века и продолжается по сегодняшний день. Ретроспективный взгляд на этот процесс позволяет выделить основные этапы её развития, связанные с наращиванием функциональных возможностей, появлением новых типов устройств и расширением области применения. На рубеже XX-XXI веков получили своё развитие интеллектуальные робототехнические системы в составе мультиагентных систем, применяемые для решения сложных задач, требующих высокой надёжности [1].

Как правило, для решения большинства задач в контексте парадигмы Интернета Вещей [2] применяются системы, сочетающие в себе комбинацию физических и информационных компонентов, такие системы получили название кибер-физические системы (КФС) [3]. Информационные компоненты используются для вычислений, исполнения алгоритмов и передачи данных через каналы связи. Физические компоненты включают в себя аналоговые элементы и различные физические устройства для взаимодействия с окружающей средой.

Для решения множества задач автоматизации и оптимизации в различных сферах человеческой жизни применяются робототехнические устройства, позволяющие сделать процесс выполнения задачи более быстрым, эффективным, безопасным для человека. С появлением большого количества доступных робототехнических устройств сформировались различные подходы к их применению, например, использование одного многофункционального робота для выполнения большого спектра задач. Подобный подход позволяет решать отдельные простые задачи, но отличается ограниченностью ресурсов и возможностей одного робототехнического устройства, что снижает эффективность и надёжность робототехнической системы в целом. При увеличении сложности выполняемых задач появляется необходимость производить расширение функционала робота и соответственно повышение сложности его структуры, увеличивается количество элементов, растет и общая стоимость робототехнического устройства. Выход из строя одной из компонент робототехнического устройства может различным образом повлиять на функционирование устройства: от снижения эффективности выполнения задач до полного выхода из строя (в случае выхода из строя источника питания). Таким образом, отказоустойчивость такой робототехнической системы обусловлена наименее отказоустойчивой компонентой этой системы.

Для эффективного решения сложных, распределённых на местности задач широкое применение получили группы взаимодействующих роботов, представляющих из себя интеллектуальные мультиагентные робототехнические системы (МРТС) [4]. Такой подход обладает рядом преимуществ перед подходом с использованием одного робота:

– автономность – при применении подхода с одним робототехническим устройством, эффективность такой системы ограничена зарядом источника питания робота. В случае выхода из строя роботу необходимо

время на восстановление, что снижает общую эффективность выполнения задач. В МРТС в случае выхода из строя одного из роботов его задачи могут быть делегированы другому роботу, способному их выполнить;

– масштабируемость – при изменении количества задач или размера территории функционирования возможно изменить количество агентов в системе без внесения изменений в принципы функционирования системы;

– надёжность – при использовании одного многофункционального робота для решения задач, надёжность такой системы будет зависеть от надёжности его различных компонентов (сенсоров, датчиков и т.д.). В МРТС используются простые в устройстве роботы, способные заменять друг друга в случае выхода из строя;

– низкая стоимость – так как роботы в МРТС просты в устройстве и способны выполнять отдельные простые задачи, они не требуют больших затрат в производстве и обслуживании;

– эффективность – существуют задачи, которые не способен выполнить один многофункциональный робот, но которые способна выполнить группа роботов, например, задачи, распределённые на местности и требующие от агентов постоянного перемещения, либо если условия окружающей среды не позволяют использование одного многофункционального робота (например, ограничения по габаритам или весу робота).

В качестве весомых аргументов в пользу применения МРТС также можно привести следующие пункты:

– отсутствие угрозы жизни и здоровью человека при выполнении различных задач, возложенных на МРТС;

– исключение человеческого фактора на этапе принятия решений системой;

– возможность потенциальной замены сложных многофункциональных дорогостоящих систем группой более простых и дешёвых робототехнических устройств.

Примеры использования МРТС. В настоящее время МРТС находят широкое применение в различных сферах деятельности человека в целях автоматизации и оптимизации выполнения тяжелой и/или опасной для человека работы. Применение МРТС позволяет автоматизировать процессы в таких сферах как производство, строительство, обслуживание складов и грузовых терминалов, аварийно-спасательные работы, работа по дому, освоение космоса, медицина, индустрия развлечений и т.д.

Примером в области развития и исследования МРТС может служить такой проект как «MARTHA» [5]. Работы над этим проектом велись в Лаборатории анализа системных архитектур Франции и его целью являлась разработка методов организации группового взаимодействия роботов для транспортировки грузов в складских помещениях. В проекте используется централизованное управление группой (от 10 до 100 шт.) роботов, управление действиями каждого робота осуществляется центральным устройством.

Другой пример централизованного управления МРТС - проект при поддержке DARPA (Defense Advanced Research Projects Agency) Министерства обороны США, выполнявшийся в Центре распределенных робототехнических систем Университета Миннесоты. В данном проекте разрабатывалось программное обеспечение и аппаратные средства для управления группой роботов-разведчиков, предназначенных для решения задач наблюдения, охраны, разведки в различных помещениях [6].

Проект «AMADEUS» был разработан в Японии и его целью являлось создание группы роботов, обеспечивающих подвоз и вывоз изделий для конвейерных линий [7]. Данный проект построен на основе децентрализованной модели управления, при которой планирование действий участников группы осуществляется несколькими устройствами.

Авторы работы [8] использовали мультиагентный подход с централизованным управлением для контроля группы из нескольких беспилотных летательных аппаратов (БПЛА). В работе описана структура системы управления, в которой присутствует оператор (человек), осуществляющий контроль над группой БПЛА с помощью человеко-машинного интерфейса. Авторы провели несколько экспериментов используя разработанную схему управления, три эксперимента были проведены с помощью симулятора и один в реальных условиях. В ходе реального эксперимента оператору удавалось успешно контролировать группу БПЛА из летящего рядом самолёта.

Существует множество других примеров проектов, построенных на основе взаимодействия группы роботов, ознакомиться с ними можно в работе [1].

Для контроля группы робототехнических устройств в МРТС могут быть использованы централизованный, децентрализованный или смешанный подходы. В работе [9] произведён обзор и анализ методов распределения задач между агентами в МРТС. При использовании централизованного управления в системе существует центральный элемент, имеющий мощный вычислительный центр, принимающий и получающий информацию от множества агентов, определяющий маршруты и распределяющий задачи между агентами-исполнителями.

При децентрализованном управлении каждый агент в системе обладает собственным вычислительным центром, способным планировать маршруты и принимать решения о выполнении задач. Во время группового позиционирования агенты обмениваются полученными знаниями через каналы связи, на их основе вносят корректировки в маршруты и разрешают конфликтные ситуации.

В случае использования смешанного подхода к управлению, существует один или несколько центральных элементов в системе, которые на основе полученной от агентов информации о местоположении, ресурсах и т.д. генерируют стратегические задачи для группы агентов-исполнителей, которые в свою очередь внутри группы с помощью децентрализованного управления решают тактические задачи.

Информационная безопасность в мультиагентой робототехнической системе. Влияние, оказываемое интеллектуальными робототехническими системами на сферы человеческой жизни с каждым годом,

увеличивается. Дешевизна и доступность элементов таких систем позволяет использовать их для широкого спектра задач, в число которых могут входить задачи, в которых важную роль играет обеспечение безопасности передаваемой между агентами системы информации. На любую информационную систему может быть совершена атака, нарушив такие важные свойства безопасности информации, как конфиденциальность, целостность и доступность, злоумышленник может снизить эффективность работы системы, получить доступ к конфиденциальной информации и использовать её в своих целях, либо полностью вывести систему из строя, нанеся ущерб владельцу такой системы. Таким образом, обеспечение безопасности информации, циркулирующей в МРТС является важной задачей для обеспечения корректной, непрерывной работы системы.

Существуют различные методы обеспечения информационной безопасности (ИБ) в МРТС. Один из подходов к обеспечению ИБ в МРТС описан в работе [10] и получил название «товарищеская модель безопасности». В данной работе авторы рассматривают уязвимости, возникающие в процессе коммуникации между агентами. Мобильные агенты делятся на несколько групп безопасности, в данных группах агенты самостоятельно отвечают за безопасность своих соседей, таким образом функция безопасности равномерно распределена между всеми агентами в системе.

Обеспечение ИБ с помощью криптографических протоколов описано в работе [11]. Автор предлагает защищённые криптографическое протоколы без использования специального доверенного субъекта в системе. Безопасность протоколов подтверждается результатами экспериментов, проведенных на реальной мультиагентной платформе.

В работе [12] авторы представили разработанный метод для обеспечения ИБ агентов, получивший название «Модель Полицейских Участков» (Police Office Model - POM). Авторы предлагают разделить территорию функционирования на регионы, в каждом из регионов присутствует агент, ответственный за безопасность этого региона, и все остальные агенты ему беспрекословно «подчиняются». Каждый мобильный агент состоит из двух частей: главной и зависимой. Главная часть ответственна за обеспечение безопасности агента, зависимая часть освобождена от этих полномочий и ответственна только за перемещение. Авторами работы [13] предложена модернизированная схема обеспечения безопасности в POM. В работе описаны механизмы авторизации и идентификации между мобильным агентом и «полицейским участком», предложен концепт сертификата подлинности агента и представлена декомпозиция процесса авторизации во времени.

Вследствие разнообразия подходов к проектированию МРТС и разнообразия используемых компонентов при производстве таких систем, проанализировав существующие подходы к обеспечению ИБ авторы пришли к выводу об отсутствии среди них универсальных. В качестве механизма обеспечения ИБ в МРТС авторами данной работы предложена усовершенствованная схема функционирования, основанная на модели полицейских участков с частично централизованным управлением.

Механизмы обеспечения безопасности. Авторы предлагают следующую схему функционирования системы. Условная территория функционирования МРТС представляет из себя прямоугольный полигон, размерность которого определяется условиями поставленных перед системой задач. Агенты системы представлены двумя типами: неподвижные роботы, задаваемые множеством $B=\{b_1, b_2, \ldots, b_m\}$, ответственные за безопасность и выполняющие роль полицейских участков. Территория функционирования системы разделена на одинаковые области – регионы, в каждом из которых располагается по одному полицейскому участку. Размер регионов определяется техническими характеристиками средств связи агентов и количеством полицейских участков. Границы регионов должны пересекаться, это необходимо для коммуникации между полицейскими участками. Второй тип агентов – подвижные мобильные роботы, представленные множеством $R=\{r_1, r_2, \ldots, r_n\}$, способные передвигаться по территории функционирования системы и выполнять поставленные задачи.

В системе присутствует два уровня информационного взаимодействия (ИВ): верхний и нижний. Верхний уровень подразумевает коммуникацию между полицейскими участками, каждый из которых обладает модулем для общения как друг с другом, так и с подвижными агентами множества B. Нижний уровень ИВ подразумевает коммуникацию между полицейскими участками и подвижными агентами. Агенты множества B имеют возможность передачи информации только полицейским участкам и не имеют возможности передавать информацию друг другу. На рис. 1 представлен пример дислокации агентов по территории функционирования.

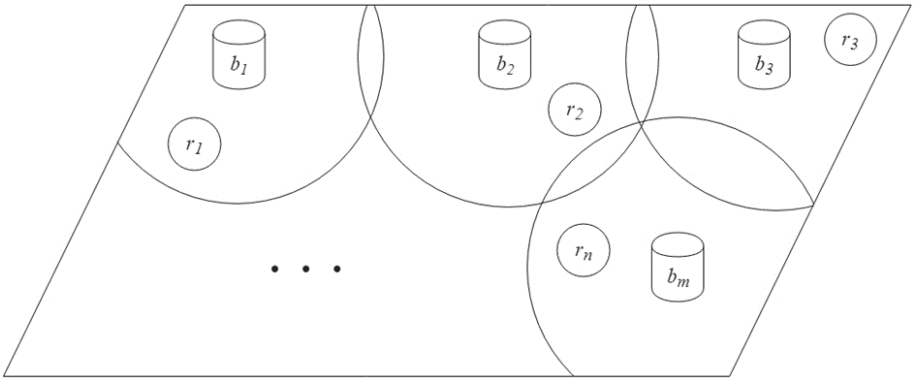


Рис. 1. Пример дислокации агентов по территории функционирования. Окружностями на схеме обозначены границы регионов

При миграции подвижного робота из одного региона в другой, он обязан установить контакт, пройти авторизацию и получить разрешение у полицейского участка, ответственного за безопасность в данном регионе. Только после этого роботу разрешается начать миграцию и, соответственно выполнение задачи. Задачи составляют множество $T=\{t_1, t_2, \ldots, t_p\}$ и подразумевают простое перемещение из одной точки в другую. Задачи распределяются полицейскими участками между подвижными роботами по схеме аукциона (задача делегируется ближайшему роботу, при условии наличия достаточного количества ресурсов для её выполнения). Обзор способов распределения задач в МРТС представлен в работе [14]. Каждый подвижный робот имеет характеристики, составляющие множество $P=\{p_1, p_2, \ldots, p_g\}$, это могут быть координаты в текущий момент времени, остаток энергоресурсов и т.д. Роботы получают информацию об окружающей среде с помощью датчиков и сенсоров.

Опишем алгоритм миграции агента при выполнении задачи. Этапы данного алгоритма схематично отображены на рис. 2.

Рис. 2. Функциональная диаграмма коммуникации между агентами

После начала функционирования системы все агенты распределены по территории случайным образом. Агент r_i, оказавшийся в регионе, контролируемом b_i, направляет b_i запрос на коммуникацию и предоставляет свой идентификатор для проверки;

b_i проверяет подлинность r_i, сверяя идентификатор с базой данных агентов. В случае успешно пройденной проверки r_i отправляет b_i данные об остатке ресурсов и текущие координаты, b_i проверяет их подлинность;

в случае успешной проверки b_i распределяет r_i задачу, формирует сертификат подлинности, основанный на характеристиках r_i и отправляет его полицейскому участку b_j, в зону действия которого r_i должен прибыть;

С этого момента r_i начинает миграцию в сторону цели. В это время b_j получает сертификат подлинности r_i от b_i. b_j проверяет существование b_i в собственном реестре полицейских участков и в случае успешной верификации сохраняет сертификат у себя;

прибыв в конечную точку маршрута r_i сообщает b_j о выполнении задачи и отправляет заявку на коммуникацию;

b_j проверяет подлинность r_i, в случае успешной проверки r_i отправляет свои данные об остатке энергоресурсов. b_j производит анализ предоставленных данных и сравнивает их с данными сертификата. В случае отсутствия расхождений b_j делегирует r_i следующую задачу.

Таким образом, в реализации ИВ на верхнем уровне отсутствует центральный управляющий объект (или центральный полицейский участок), агент b_i принимает решения относительно агентов, находящихся в его регионе. Полицейские участки обмениваются информацией о роботах-нарушителях и совместно принимают решения об их блокировке, и взаимодействуют при передаче управления роботом r_i от b_i к b_j.

Заключение.

Предложенная авторами схема функционирования мультиагентной робототехнической системы позволяет добиться обеспечения таких свойств безопасности информации как целостность и доступность. При этом, обеспечения конфиденциальности можно добиться за счёт внедрения в схему криптографических алгоритмов для шифрования передаваемой между агентами информации. Перспективным решением проблемы конфиденциальности в контексте мобильных робототехнических систем видится использование алгоритмов квантового распределения ключей шифрования между агентами. Фундаментальные принципы квантовой физики утверждают, что при генерации квантового ключа злоумышленник, пытающийся внедриться в канал связи, будет в любом случае обнаружен. В будущих исследованиях авторами планируется анализ поведения системы в условиях деструктивного информационного воздействия со стороны злоумышленников, разработка схемы функционирования с использованием квантового шифрования, разработка программного симулятора для проведения экспериментов и анализа эффективности работы системы с используемыми механизмами обеспечения информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Каляев И. А., Гайдук А. Р., Капустян С. Г. Модели и алгоритмы коллективного управления в группах роботов. Монография. – 2009.
2. Ястреб Н. А. Четвертая промышленная революция: глобальные промышленные сети и Интернет вещей //ИнВестРегион. – 2014. – №. 4. – С. 22.
3. Wolf W. H. Cyber-physical systems //IEEE Computer. – 2009. – Т. 42. – №. 3. – С. 88-89.
4. Ganguli A. et al. On collective motion in sensor networks: sample problems and distributed algorithms //Decision and Control, 2005 and 2005 European Control Conference. CDC-ECC'05. 44th IEEE Conference on. – IEEE, 2005. – С. 4239-4244.
5. Alami R. et al. Multi-robot cooperation in the MARTHA project //IEEE Robotics & Automation Magazine. – 1998. – Т. 5. – №. 1. – С. 36-47.
6. Rybski P. E. et al. System architecture for versatile autonomous and teleoperated control of multiple miniature robots //Robotics and Automation, 2001. Proceedings 2001 ICRA. IEEE International Conference on. – IEEE, 2001. – Т. 3. – С. 2917-2922.
7. Kamada T., Oikawa K. AMADEUS: a mobile, autonomous decentralized utility system for indoor transportation //Robotics and Automation, 1998. Proceedings. 1998 IEEE International Conference on. – IEEE, 1998. – Т. 3. – С. 2229-2236.
8. Baxter J. W., Horn G. S., Leivers D. P. Fly-by-agent: Controlling a pool of UAVs via a multi-agent system //Knowledge-Based Systems. – 2008. – Т. 21. – №. 3. – С. 232-237.
9. Yan Z., Jouandeau N., Cherif A. A. A survey and analysis of multi-robot coordination //International Journal of Advanced Robotic Systems. – 2013. – Т. 10. – №. 12. – С. 399.
10. 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.
11. Tate S. R. Mobile agent security through multi-agent cryptographic protocols : дис. – UNIVERSITY OF NORTH TEXAS, 2004.
12. Guan, X., Yang, Y., & You, J. (2000, May). POM-a mobile agent security model against malicious hosts. In hpc (p. 1165). IEEE.
13. Zikratov I. A. et al. Securing swarm intellect robots with a police office model //Application of Information and Communication Technologies (AICT), 2014 IEEE 8th International Conference on. – IEEE, 2014. – С. 1-5.
14. Dias M. B. et al. Market-based multirobot coordination: A survey and analysis //Proceedings of the IEEE. – 2006. – Т. 94. – №. 7. – С. 1257-1270.

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ

УДК 519.8

СОДЕРЖАТЕЛЬНАЯ И ФОРМАЛЬНАЯ ПОСТАНОВКА ЗАДАЧИ ПЛАНИРОВАНИЯ ТЕХНИЧЕСКОГО ПЕРЕВООРУЖЕНИЯ ПРОМЫШЛЕННОГО ОБЪЕКТА

Захаров Валерий Вячеславович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: valeriov@yandex.ru

Аннотация. Определено место задачи технического перевооружения промышленного объекта в процессе его модернизации. Проведено описание задачи планирования технического перевооружения в сложных организационно-технических системах. Обосновано применение логико-динамических моделей для решения подобных задач.

Ключевые слова: комплексное моделирование; логико-динамический подход; планирование; техническое перевооружение, промышленные социо-киберфизические системы.

FORMAL AND NOTIONAL PROBLEM'S DESCRIPTION OF PLANNING AN INDUSTRIAL FACILITY'S TECHNICAL REEQUIPMENT

Zakharov Valerii
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th liniya, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: valeriov@yandex.ru

Abstract. The task's place of industrial facility's technical re-equipment was determined in the process of its modernization. The description of planning a technical reequipment in complex organizational and technical systems' problem was conducted. The application of logical-dynamic models for solutions of such problems was grounded.

Keywords: complex simulation; logical-dynamic approach; planning; technical re-equipment of production.

В современных условиях конкурентной борьбы и импортозамещения вопрос модернизации, направленной на обеспечение стабильного функционирования производственных комплексов устойчиво занимает лидирующее положение в повестке любого промышленного форума. Средняя степень износ основных фондов в обрабатывающем производстве, строительстве, транспортировке и хранении в РФ по данным 2017 года превышает 50% [1]. Для выхода местных продуктов на мировые рынки требуется добиться существенного повышения качества и технического уровня продукции предприятий во всех отраслях народного хозяйства. Стоит задача коренной реконструкции и модернизации производственных комплексов, а также обеспечение опережающих темпов развития в области машиностроения, обрабатывающем производстве, строительстве. Полный и единовременный отказ от устоявшихся подходов к производству и управлению, форсированные изменения и слепое следование трендам опасно. Особое внимание сегодня уделено проблемам технического перевооружения(ТП) промышленного объекта, обеспечивающего повышение производительности труда и сокращение издержек. Решения подобных задач не сводится к простой замене оборудования, а требуют проведения инновационного или интенсивного перевооружения, т.е. перехода к качественно новому уровню производства и выпуска продукции.

Модернизация в эпоху четвертой промышленной революции - это замена старых машин, механизмов и оборудования на более производительное с целью привлечения новых заказов, клиентов, а также формирование производственных социо-киберфизических систем (ПСКФС) для управления взаимосвязанными физическими объектами, вычислительными мощностями и персоналом с помощью умных устройств и сенсоров. В настоящий момент актуальной задачей является оптимизация жизненных циклов изделий и процесса создания производственных комплексов будущего [2].

Очевидно, что предприятия сегодня функционируют на высококонкурентных пространственно и временно распределенных мировых рынках. Подобная децентрализация производств и сбыта является причиной существенной неопределенности среды. Временные задержки и ошибки в управлении, вызванные неверным решением задачи анализа состояний и формирования управляющих воздействий могут привести к необратимым негативным последствиям. Принятие оптимальных по срокам, критериям точности и обоснованности оперативных

и стратегических производственно-управленческих решений в системах характеризующими исключительной сложности, является залогом успешного функционирования.

ПСКФС от традиционных технических систем, систем реального времени и сенсорных сетей отличает: вычислительный потенциала в каждом физическом компоненте системы, высокая степень автоматизации; сетевое взаимодействие; поддержка интеграции при пространственном и временном масштабировании; возможность динамической реконфигурации как на информационном, так и на физическом уровнях [3]. Глобальных целей функционирования промышленного объекта может быть несколько, кроме того они изменчивы во времени. Очевидно, что их невозможно достичь одновременно, поскольку зачастую обладают диалектической противоречивостью. Система должна стремиться с наименьшими затратами ресурсов достичь области достижимости, однако и она динамична и изменяется в каждый момент времени из-за внутренних и внешних факторов. Цель функционирования ПСКФС: оперативный, т.е. своевременный синтез и выбор обоснованных вариантов упреждающего управления направленного на достижение области в каждый момент времени из множества допустимых альтернатив при минимальных затратах. Основной целью внедрения ПСКФС является повышение эффективности формируемых управляющих воздействий [4], преодолевающих возмущения среды и неопределенности.

Практика диктует необходимость оперативной разработки и внедрения процедур, моделей, методов, алгоритмов и методик проактивного интеллектуального мониторинга и управления производственными и информационными процессами при котором обнаружение и ликвидация сбоев и отказов в нештатных ситуациях будет происходить значительно раньше, чем станут проявляться возможные негативные последствия. Другими словами, применение постоянно совершенствующих инструментов и информационных технологии является неотъемлемым атрибутом современных и будущих технологических и управленческих процессов в производственных комплексах.

Обратим внимание на изменившуюся среду в которой функционирует промышленный объект. Темпы научно-технического прогресса, развития микроэлектроники и информационных технологий, возросли до такой степени, что потенциал функциональных возможностей новых разработок опережает сроки внедрения предыдущих разработок [5]. На практике мы видим устаревшие системы не способные оперативно и информативно отображать и передавать данные пользователю по надежным и защищенным каналам. Данное явление принято называть моральным износом. Описанный ранее вид износа ПСКФС проявляется в тот момент начала преображения структура спроса по причине изменений потребительских требований к составу и качеству выпускаемого продукта из-за появления новых разработок в производственной и информационной сфере. В процессе планирования, проектирования, эксплуатации и модернизации ПСКФС остро стоит необходимость прогнозирования показателей моральной долговечности её элементов.

Вероятным решением описанной выше проблемы является построение гибко и оперативно функционально развиваемой(адаптивной) модульной системы на основе сервис-ориентированной архитектуры и опережающая модернизация, при разрешение диалектического противоречия в виде осуществления инновационной деятельности и автоматизации хорошо изученных и стабильных бизнес-процессов [5]. Очевидно, что требуется определение оптимальных темпов и сроков проведения работ в подсистемах где они увеличивают потенциал системы посредством повышения общей эффективности функционирования.

Для решения задачи повышения адаптивности в проектируемую систему необходимо заложить производственную и вычислительную избыточность, рассчитанную на дальнейший рост потребностей в информационном и производственном обеспечение. Подобным моделям характерно наличие дополнительных изменяемых настроек оборудования и конфигураций структуры в целом. На физическом уровне должна быть возможность осуществления реконфигурации контроллеров и установка независимых от элементов системы датчиков и измерительных приборов [6]. На информационном уровне следует создать возможность динамически изменять информационное пространство [7]. Описанное требование системообразующее, поскольку обмен информации в ПСКФС основа её функционирования [8]. Подобная адаптивная система, обладает свойством приспособления к изменяющимся в определенных границах условиям [9].

Сегодня требуется составлять такой планы замены, ремонта и внедрения оборудования на промышленных объектах который обеспечивает минимум суммарных приведенных затрат на создание и развитие новой производственной структуры предприятия с учетом динамики спроса, изменении физического и морального износа при ограничениях на выделяемые материальные, трудовые ресурсы и возможности освоения капитальных вложений. Замена должна быть осуществляться таким образом, чтобы, с одной стороны, поставки продукции предприятия для клиентов не уменьшались, а с другой, внедрение новых машин, технологий и их отладка с запуском не влияли на поставщиков и работу собственных производственных мощностей. Рыночные условия диктуют необходимость в планах, исключающих прерывания и уменьшение производительности, а также сохраняющем согласованные обязательства и взаимосвязанные процессы при минимальных издержках. Внедрение инструментов мониторинга и управления технологическими процессами требует тщательного планирования. Модернизация состоит из следующих шагов: синтез облика текущей производственной структуры, синтез оптимальной производственной структуры, определение сроков модернизации, синтез технологии модернизации, синтез плана модернизации [10].

Строго говоря, выбор адекватных подходов к модернизации в первую очередь зависит от полноты и достоверности входных данных. Количество связей, уровней управления и применение информационных технологий, а именно использование интегрированных систем мониторинга производства, управления запасами,

продажами, бухгалтерией и финансами указывает на то, что современное предприятие является сложным организационно-техническим объектом (СОТО). Моделирование устойчивых пространственно и временно распределенных производственно-управленческих решений и описание ограничений на потребляемые ресурсы с соответствующими взаимосвязями предполагает многоуровневое представление данной структуры.

Задачи предполагают применение полимодельного многокритериального описания с использованием комбинированных методов, алгоритмов и методик, позволяющих обеспечить эффект конструктивного, но не избыточного научного-методологического исследования свойств и состояний промышленного объекта в реальном времени [10,11]. Целесообразно в первую очередь осуществить синтез новой ПСКФС, а затем выполнить описание текущего состояния в определенных концептах, определить сроки, технологии и разработать план модернизации.

Синтез глобальной структуры ПСКФС или синтез верхнего уровня представляет собой оптимизацию упорядоченного множества подсистем и модулей промышленного объекта. Синтез нижнего уровня - это создание контура управления для формирования управляющих воздействий при локальной стационарности структуры ПСКФС. Контур управления (КУ) системами строится с опорой на доступную информацию, поэтому искомый алгоритм зависит от состава применяемых измерителей. КУ характеризуется в том числе и отражением свойств управляемых подсистем [4].

Управление оперативно настраиваемыми многофункциональными группами машин по мнению автора является базовым. Именно оптимальное управление подобными системами позволяет на меньшем количестве производственных мощностей выпускать значительно индивидуализированный под заказ потребителя продукт высокого качества в любом объеме, сохраняя заданную рентабельность и экономическую эффективность производства в целом [12].

Как было сказано выше, одной из задач проектирования ПСКФС является снижение сложности промышленного объекта с сохранением обоснованности принимаемых решений, при соблюдении требований к управляемости, надежности, наличию оптимизационного потенциала, информационной безопасности. Сложность ПСКФС определяется количеством входящих в неё подсистем: информационных, технических, а также их взаимодействием. Относительно конкретных целей промышленного объекта система может быть неполной, избыточной и полностью соответствующей поставленным задачам. Избыточности проектируемой ПСКФС должна быть обоснована математически, кроме того должны выполняться требования опережающего развития.

Эффективность принимаемых решений снижается в условиях старения информации. Сегодня повышаются требования к качеству проактивного интеллектуального мониторинга, скорости формирования возможных альтернатив и реализации выбранного управления. Это связано с тем, что именно на нижних уровнях и этапе реализации плана производства происходит формирование конечной стоимости с точки зрения потребителя продукции по показателям: срок, цена, качество. Здесь эталонный план подвергается воздействиям, источником которых является неопределенности как внешней, так и внутренней среды.

Проектирование оптимальной ПСКФС следует начинать с синтеза структуры и архитектуры нижнего уровня. Он заключается в обоснованном выборе состава производственных машин, механизмов и измерительных приборов, т.е. синтезе структуры и архитектуры производственных и вычислительных мощностей. На практике - это комплекс мероприятий по повышению технико-экономического уровня отдельных производств, цехов, участков, техники и технологий, механизации и автоматизации производств, замена морально и физически изношенного оборудования, другими словами ТП. Решение задачи перевооружения является первым этапом модернизации промышленных объектов.

ТП характерны научно-технические проблемы двух родов. К первому роду относятся согласование применяемых моделей, методов и алгоритмов на концептуальном, модельно-алгоритмическом, информационном, программно-управленческих уровнях. Проблемы второго рода связаны с задачами структурного синтеза облика: размерность, нелинейность, учет неопределенностей, многокритериальная оптимизация на полимодельном уровне. Данные проблемы характерны для каждого уровня ПСКФС, однако на нижних уровнях решений существенно больше. Чем выше в иерархической пирамиде находится решение, тем меньше связей, элементов и критериев оптимизации следует учитываться в контуре управления. Подобный подход упростит систему и повысит скорость синтеза области допустимых решений, однако снизит их обоснованность.

На каждой ступени в иерархии КУ свои особенности, невозможно с помощью унифицированного подхода сформировать отдельно все уровни в ПСКФС, ведь для них характерны отличные друг от друга акты решений, что определяет необходимость в применении системного подхода. Следует помнить, что чем проще метод синтеза, тем сложнее процесс разработки подходящего для этого метода модели и объем потребляемых ресурсов [9].

Производства будущего предоставят возможности потребителю “on-line” сформировать уникальный по своим характеристикам продукт. Удаленно использовать распределенные мощности промышленных компаний, по аналогии с арендой вычислительных мощностей и серверов сегодня. Анализ показал, что преодоление перечисленных проблем на всех уровнях и плавный переход к гибким, адаптивным, самоорганизующимся автоматизированным производительным предприятиям, реагирующим на изменяющиеся требования рынка, станет возможен только при использовании комплексного подхода, базирующегося на фундаментальных и прикладных результатах, полученных на междисциплинарном уровне. Отрасли системных знаний, прежде всего такие научные направления, как системология, неокибернетика и информатика являются базой для подобных исследований. Необходимо провести динамическую интерпретация классических задач исследования операций, в рамках которой происходит обоснованный выбор траекторий перевооружения.

Планирование ТП следует интерпретировать как этап программного управления техникой и технологическим оборудованием с целью перевода их в заданное многоструктурное макросостояние. Ряд исследований показал, что возможный вариант формального описания процессов управления структурной динамикой СОТО базируется на логико-динамических моделях (ЛДМ). Они обладают следующими достоинствами: позволяют использовать результаты, полученные в современной теории управления сложными динамическими системами с перестраиваемой структурой; применение позволяет сокращать размерность задач планирования; обеспечивают согласование и взаимную интерпретацию результатов, полученных как на аналитических и имитационных моделях планирования, так и на концептуальном, алгоритмическом, информационном и программном уровнях описания; позволяют обоснованно выбирать временные интервалы работы элементов и подсистем [12]. Использование векторов показателей качества управления операциями, ресурсами и потоками, а также ограничений, оказывающих влияние на соответствующие зависимые модели, является одним из достоинств данного класса моделей, которое позволяет обоснованно осуществлять управленческо-динамическую интерпретацию производственных процессов и ТП в СОТО [13].

Дальнейшую работу следует направить на анализ существующих подходов к проектированию ПСКФС и их интеграции в процесс функционирования предприятий. Необходимо разработать методы синтеза структуры ПСКФС и контура управления подобными системы и их оценки.

Исследования, выполненные по данной тематике, проводились при финансовой поддержке ведущих университетов Российской Федерации: СПб ГПУ (мероприятие 6.1.1), ИТМО (субсидия 074–U01), грантов РФФИ (№№ 16-07-00779, 16-08-00510, 16-08-01277, 16-29-09482-офи-м, 17-08-00797, 17-06-00108, 17-01-00139, 17-20-01214, 17-29-07073- офи-м, 18-07-01272, 18-08-01505), Госзадания Министерства образования и науки РФ №2.3135.2017/4.6, в рамках бюджетных тем №№0073–2018–0003 (№ гос. регистр. АААА-А16-116030250074–1), Международного проекта ERASMUS+, Capacity building in higher education, №73751-EPP-1-2016-1-DE-EPPKA2-CBHE-JP, Новые стратегии обучения инженеров с использованием сред визуального моделирования и открытых учебных платформ.

СПИСОК ЛИТЕРАТУРЫ

1. Россия в цифрах 2018: Крат.стат.сб./Росстат-М., Р76 2018 -522 с.
2. Гурьянов А.В., Заколдаев Д.А., Шукалов А.В., Жаринов И.О., Костишин М.О. Организация цифровых производств Индустрии 4.0 на основе киберфизических систем и онтологий // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 2. С. 268–277.
3. Miclea L., Sanislav T. About dependability in cyber-physical systems // Design & Test Symposium (EWDTS): 9th East-West. IEEE. 2011. P. 17—21
4. Морозов В.П., Дымарский Я.С. Элементы теории управления ГАП: Математическое обеспечение. - Л.: Машиностроение, Ленингрдское отдние, 1984 - 333с.
5. Юсупов Р.М., Мусаев А.А. Проблема оценивания эффективности информационных технологий. Материалы конференции «Информационные технологии в управлении» (ИТУ-2018). СПб.: АО «Концерн «ЦНИИ «Электроприбор», 2018. 742 с.
6. Miclea L., Sanislav T. About dependability in cyber-physical systems // Design & Test Symposium (EWDTS): 9th East-West. IEEE. 2011. P. 17—21
7. Tetsuo Tomiyama, Florioan Moyen Resilient architecture for cyber-physical production systems. CIRP Annals - Manufacturing Technology 2018, Pages 161-164
8. Ронжин А. Л., Басов О. О., Соколов Б. В., Юсупов Р. М. Концептуальная и формальная модели синтеза киберфизических систем и интеллектуальных пространств // Изв. вузов. Приборостроение. 2016. Т. 59, № 11. С. 897—905.
9. Микони С. В., Соколов Б. В., Юсупов Р. М. Применение алгебраического подхода в квалиметрии моделей и полимодельных комплексов // Сборник докладов VI научно-практической конференции «Имитационное моделирование. Теория и практика». — Казань: Фэн, 2013. — Том 1. — С. 68–79.
10. Охтилев М.Ю., Соколов Б.В. Юсупов Р.М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. - М.: Наука, 2006. – 410с.
11. Жашкова Т.В. Процедура идентификационно-структурного синтеза моделей для анализа критических состояний сложных систем // Современные проблемы науки и образования. – 2013. – № 6.
12. Попов Е.П. Робототехника и гибкие производственные системы. - М.: Наука. Гл. ред. физ.-мф. лит., 1987. - 192 с
13. Потрясаев С. А. Комплексное моделирование сложных процессов на основе нотации BPMN // Изв. вузов. Приборостроение. 2016. Т. 59, № 11. С. 913—920.

УДК 519.711

ПОСТРОЕНИЕ И АППРОКСИМАЦИЯ ОБЛАСТЕЙ ДОСТИЖИМОСТИ: ОБЗОР СУЩЕСТВУЮЩИХ РЕШЕНИЙ И ВЫБОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Ушаков Виталий Анатольевич
Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: mr.vitaly.ushakov@yandex.ru

Аннотация. Рассмотрены существующие решения (программное обеспечение) для построения и аппроксимации областей достижимости. Выполнен анализ и выбор решения для построения областей достижимости.

Ключевые слова: область достижимости; построение областей достижимости; аппроксимация областей достижимости; целевое множество.

REACHABILITY AREA CONSTRUCTION AND APPROXIMATION: REVIEW EXISTING SOLUTIONS AND A CHOICE OF SOFTWARE

Ushakov Vitaly
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th liniya, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: mr.vitaly.ushakov@yandex.ru

Abstract. The existing solutions (software) for the construction and approximation of reachability areas are considered. The analysis and choice of solutions for the construction of reachability areas.

Keywords: reachability area; reachability area construction; approximation area construction; target set; Matlab; Mathematica.

Введение.

На практике при решении задач оптимального управления сложными техническими объектами (СТО), имеющими иерархически-сетевую структуру, возникают существенные трудности, вызванные большой размерностью указанных задач, сложным характером ограничений на процесс управления, существенной нелинейностью математических моделей, описывающих функционирование реальных динамических систем. В этих условиях особую актуальность приобретает задача повышения оперативности и обоснованности принятия управленческих решений, связанных с конфигурированием (реконфигурированием) структур автоматизированных систем управления (АСУ) летательными аппаратами (ЛА), основанных на построении и аппроксимации множеств достижимости логико-динамических моделей указанных автоматизированных систем, описывающих данную предметную область в динамически изменяющихся условиях [1]. Но для решения данной задачи, в первую очередь, необходимо выполнить построение области достижимости (ОД) АСУ ЛА.

Знание ОД дает максимальную информацию о возможностях рассматриваемой автоматизированной системы. Например, на основе ОД можно оценить, с одной стороны, пропускные способности АСУ ЛА (интегральную, дифференциальную пропускную способность), с другой стороны, маневренные возможности ЛА, выбрать оптимальную программу управления, формировать оптимальное управление при наведении ЛА и т.д.

В современной теории управления существует множество задач, в ходе решения которых возникает потребность в построении и анализе ОД управляемой системы [2]. По существу, методы построения ОД можно разделить на два подхода. Первый подход заключается в построении точных ОД, охватывающих только те состояния динамической системы, в которые она может быть переведена за конечный промежуток времени. Второй подход подразумевает построение некоторой аппроксимации ОД [3], например, с помощью эллипсоидов [2]. Аппроксимационным методам в настоящее время уделяется большое внимание [2, 3], поскольку они позволяют значительно сократить вычислительные затраты. Однако аппроксимационные методы дают лишь приближенное представление о ОД, которое в некоторых случаях является весьма грубым.

Обзор существующих решений (программного обеспечения) для построения и аппроксимации ОД.

Нами проведен обзор существующих решений (программного обеспечения) для построения ОД. Далее представлены наиболее интересные из них.

В [4] предложен численный алгоритм для построения ОД нелинейной системы с импульсным управлением. В [5] рассматривается задача приближенного построения ОД динамической системы и численные методы решения этой задачи на кластерных вычислительных системах, графических процессорных устройствах и нейросетевых ускорителях. В указанной работе приведен пример построения ОД ЛА в графическом процессорном устройстве NVIDIA GeForce 9600 GT. В качестве среды разработки была выбрана Microsoft Visual Studio 2008 и технология OpenCL. На рис. 1. [5] в качестве примера показана ОД ЛА при двух стационарных сферических препятствиях.

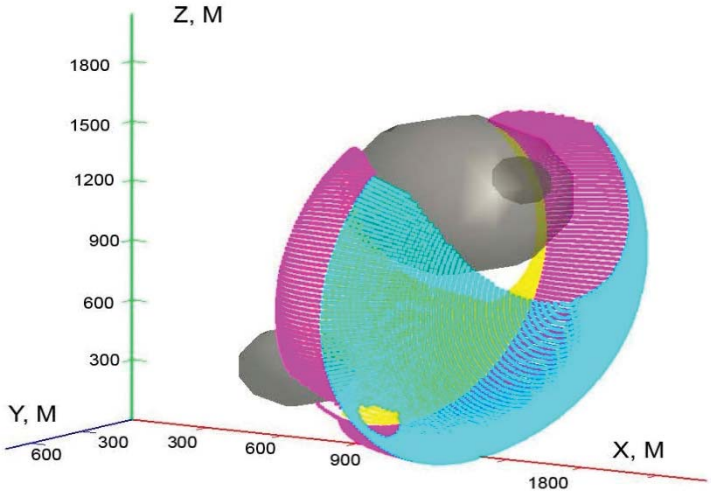


Рис. 1. ОД ЛА при двух стационарных сферических препятствиях

В [6, 7] рассматривается построение ОД линейных дискретных динамических систем на основе модифицированного общего рекуррентного алгебраического метода. В указанных работах приведены примеры моделирование ОД системы в программном пакете Matlab 8.4 (R2014b). На рис. 2. [6] показан результат численного моделирования областей достижимости динамической системы. На рис. 3. [7] показан результат построения выпуклых оболочек типовых видов множеств в $\mathbb{R}^2$.

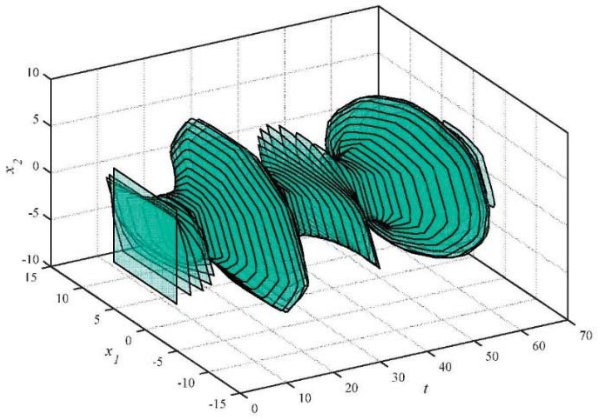


Рис. 2. Области достижимости системы

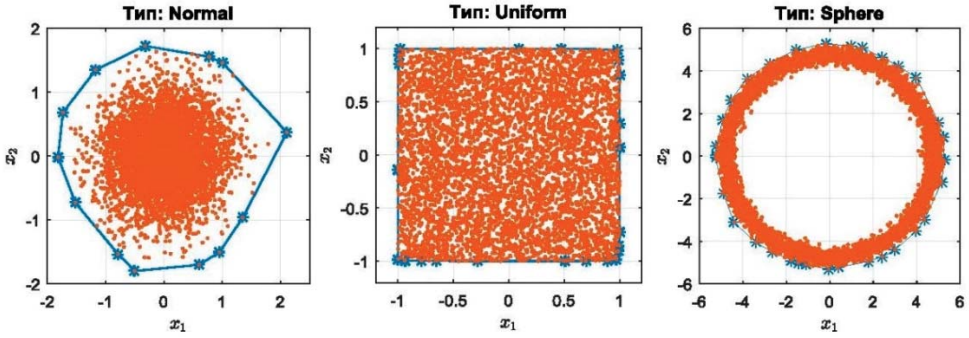


Рис. 3. Выпуклые оболочки типовых видов множеств в $\mathbb{R}^2$

В [8] рассматривается задача сравнения ОД непрерывной нелинейной и линеаризованной дискретной управляемых динамических систем. В качестве объекта управления используется модель ЛА, движение которого описывается системой нелинейных динамических уравнений. В указанной работе приведен пример моделирования алгоритма аппроксимации ОД нелинейной модели ЛА в программной среде Matlab R2014a. На рис. 4. [8] показан результат моделирования ОД нелинейной и линеаризованной системы.

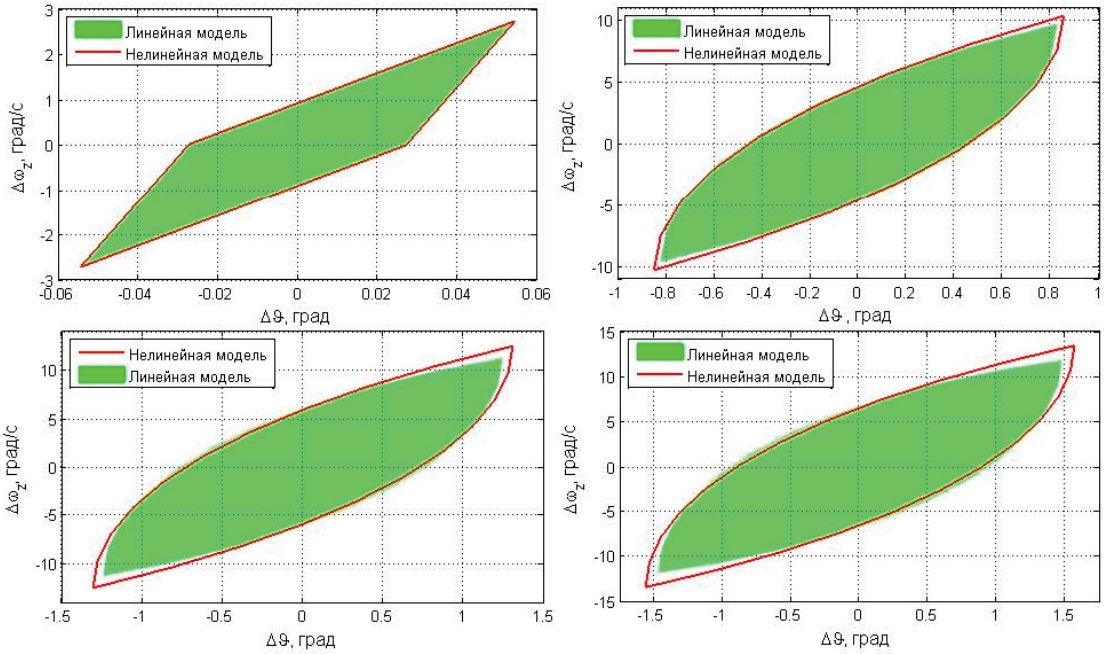


Рис. 4. Пример аппроксимации нелинейной и линейной моделей

В [9] рассматривается линейная стационарная система третьего порядка с одним управляющим (возмущающим) воздействием, ограниченным по абсолютной величине. В качестве объекта управления используется модель ЛА, движение которого описывается системой нелинейных динамических уравнений. В указанной работе приведен пример построения ОД в пакете Mathematica с помощью матричного уравнения с управляющими функциями, который показан на рис. 5 [9].

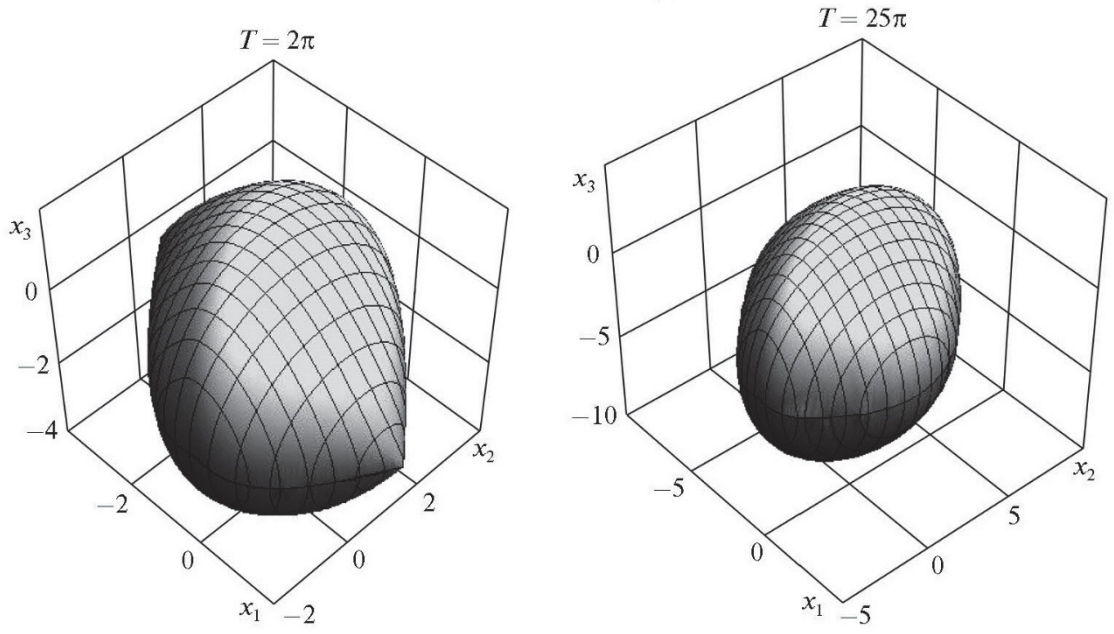


Рис. 5. Пример построения ОД в пакете Mathematica

Очевидно, что используется различное программное обеспечение для построения ОД – Matlab, Mathematica и языки программирования высокого уровня (ЯП ВУ). Однако, можно сделать однозначный вывод о том, что большинство существующих решений для построения ОД в различных системах и на основе различных алгоритмов выполняются в Matlab. Кроме того, следует помнить, что как отмечено во введении – самым распространенным способом является аппроксимация ОД, т.е. приближенное построение ОД.

Выбор программного обеспечения (ПО) для построения ОД.

В условиях постоянно растущей сложности решаемых научных задач актуальным становится применение средств вычислительной техники для проведения расчетных операций. При этом требуется построение компьютерных моделей, реализующих различные методы решения математических задач.

Из проведенного в предыдущем разделе обзора, становится ясно, что существующие подходы не удовлетворяют требованиям, предъявляемым к уровню детализации и качеству решения исследуемых задач управления конфигурацией (реконфигурацией) структур АСУ ЛА. Эти требования связаны, во-первых, с необходимостью проецирования целевого множества на ОД [10]. Во-вторых, существует четыре варианта взаимного расположения выпуклой оболочки и ОД АСУ ЛА, которые надо детально исследовать для различных сценариев изменения внешних и внутренних возмущающих воздействий [10, 11].

Учитывая описанное выше, необходимо обосновать выбор базового ПО для решения поставленной задачи. В качестве основных вариантов остановимся на таком ПО, как Matlab, Mathematica, MathCad и ЯП ВУ. Результаты проведенного анализа для выбора среды разработки (построение ОД) приведены в таблице 1.

Таблица 1

Сравнение сред для решения задачи построения ОД

Критерии отбора	Matlab	Mathematica	MathCad	ЯП ВУ
Бесплатное распространение	–	–	–	+
Простота разработки	+	+	+	–
Простота использования	+	–	–	+
Разработка без знания ЯП ВУ	+	+	+	–
Простота расширения	+	+	–	–

Поясним, что под «простотой разработки» понимается легкость разработки системы для эксперта, «простота использования» – легкость использования конечным пользователем (наличие хорошего графического интерфейса), «простота расширения» – легкость и возможность быстрой разработки дополнительных модулей. Как видно из таблицы 1 – самым перспективным является использование Matlab несмотря на то, что он распространяется только на платной основе. Кроме того, очевидно, что главным критерием для выбора ПО является визуализация результатов моделирования, что на наш взгляд лучше всего реализовано в Matlab. А также, абсолютно ясно, что использование существующих математических пакетов прикладных программ (ППП) является наиболее предпочтительным методом моделирования и решения поставленных исследовательских задач.

Заключение.

Рассмотрены существующие подходы к решению задач построения и аппроксимации ОД СТО (в том числе и АСУ ЛА). Ясно, что используется различное ПО для построения ОД – Matlab, Mathematica и ЯП ВУ. Однако, с учетом выполненных исследований можно сделать вывод о том, что большинство существующих решений, связанных с построением ОД в различных системах и на основе различных алгоритмов выполняются в инструментально-программной среде Matlab. Выполнен анализ и выбор решения для построения и аппроксимации ОД с использованием ППП.

Исследования, выполненные по данной тематике, проводились при частичной финансовой поддержке госбюджетной темы № 0073-2018-0003.

СПИСОК ЛИТЕРАТУРЫ

1. Ушаков В.А. Автоматизированные системы управления подвижными объектами // XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)»: Материалы конференции (СПб, 24-26 октября 2018 г.). СПб.: СПОИСУ –2018. С. 589.
2. Черноусько Ф.Л. Оценивание фазового состояния динамических систем. Метод эллипсоидов. М.: Наука, 1988. 320 с.
3. Потрясаев С.А. Динамическая модель и алгоритмы комплексного планирования операций и распределения ресурсов в корпоративной информационной системе: Дисс. ... канд. техн. наук: 05.13.01: СПб., 2009. 159 с.
4. Вдовина О.И., Сесекин А.Н. Численное построение областей достижимости для систем с импульсным управлением // Труды Института математики и механики УрО РАН. 2005. Т 11, №. 1, С. 65-73.
5. Быстров А.В., Карпенко А.П., Козлова О.Г., Федин В.А. Система поддержки принятия решений при выборе параллельного аппаратно-программного комплекса для построения областей достижимости летательного аппарата // Параллельные вычислительные технологии (ПАВТ'2011). М.: Издательский центр ЮУрГУ, 2011. С. 60-68.
6. Булаев В.В., Осипов И.О. Модифицированный алгоритм построения областей достижимости линейных дискретных динамических систем // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. 2018. Т 18, №. 1, С. 56-62.
7. Булаев В.В., Осипов И.О. Об одном модифицированном рекуррентном алгебраическом методе построения областей достижимости линейных дискретных динамических систем // Ракетно-космическая техника. 2017. Т 1, №. 2(10), С. 4-15.
8. Горанов А.Ю., Шориков А.Ф. Анализ точности общего алгебраического метода построения областей достижимости линеаризованных динамических систем // Труды второй научно-технической конференции молодых ученых уральского энергетического института. Екатеринбург: УрФУ, 2017. С. 407-410.
9. Бугров Д.И., Формальский А.М. Зависимость от времени областей достижимости систем третьего порядка // Прикладная математика и механика. 2017. Т 81, №. 2, С. 154-164.
10. Губанов В.А., Захаров В.В., Коваленко А.Н. Введение в системный анализ: Учеб. пособие/Под ред. Л.А. Петросяна. Л.: Издательство Ленинградского университета, 1988. 232 с.
11. Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. М.: Наука, 2006. 410 с.

УДК 004.72 + 621.391

МЕТОД СИНТЕЗА МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ

Журавель Евгений Павлович
Санкт-Петербургский политехнический университет Петра Великого
Политехническая, ул., 29, Санкт-Петербург, 195251, Россия
e-mail: eshur2003@mail.ru

Аннотация. Предложен метод структурно-параметрического синтеза позволяющий формировать мультисервисную сеть связи, обладающую заданными характеристиками её функционирования.

Ключевые слова: структурно-параметрический синтез; мультисервисная сеть связи.

METHOD OF SYNTHESIS OF A MULISERVICE COMMUNICATION NETWORK

Zhuravel Evgeny
Peter the Great St.Petersburg Polytechnic University,
29 Polytechnicheskaya St, St.Petersburg, 195251, Russia
e-mail: eshur2003@mail.ru

Abstract. The method of structural and parametric synthesis allowing to create the multiservice communication network possessing the given characteristics of its functioning is offered.

Keywords: structural and parametric synthesis; multiservice communication network.

В процессах жизненного цикла (ЖЦ) мультисервисной сети связи (МССС) разрабатываются, оцениваются, принимаются и реализуются решения по проектированию, построению, реконструкции, развитию и эксплуатации структуры МССС, каждое из которых характеризуется набором и значениями параметров МССС, а также их стоимостью. Эти процессы ЖЦ МССС представляют собой, по сути, итерационное решение задачи синтеза её структуры (точек присутствия организации связи, видов, количества, взаимосвязей и размещения телекоммуникационного оборудования (ТКО), видов и количества линий связи, разработки и (или) доработки высокоуровневого и (или) низкоуровневого дизайна сети связи и пр.) на основе информации об используемых и (или) планируемых к использованию элементах пассивного и активного ТКО и требуемых значениях параметров функционирования МССС. Выработка вариантов решений синтеза структуры фиксированных МССС осуществляется с учетом краткосрочных (до одного года) и среднесрочных (от одного до трех лет) горизонтов планирования эксплуатации и развития МССС и предоставляемых ими услугах. К МССС могут быть предъявлены требования по достижению требуемых значений характеристик её функционирования в максимально сжатые временные сроки. В связи с этим, выявляется противоречие между существующими подходами к решению задач реконструкции, развития и эксплуатации МССС и требованиями к решению этих задач в установленные сроки, а также научному и техническому обоснованию их результатов и требуемых ресурсов. Разрешение данного противоречия возможно путём наиболее полного использования потенциальных возможностей пассивного и активного ТКО МССС на основе принципов автоматизации управления при построении МССС, применение которых обусловлено как высокой размерностью характеристик ТКО, так и высокой сложностью процессов функционирования МССС.

Исходя из приведенных выше рассуждений в [1] рассмотрена обобщенная задача синтеза МССС, решаемая на этапах проектирования, построения, реконструкции, развития и эксплуатации её жизненного цикла. Решение обобщённой задачи структурно-параметрического синтеза МССС в соответствии с формулируемым подходом [1] и методом последовательных уступок [2] заключается в следующем. Для очередного выбранного по предпочтительности критерия в рамках имеющегося значения уступки ранее решенной задачи выполняется нахождение рациональной, на данном этапе структуры подсети МССС. Для достижения требуемого значения интегрального показателя результатов функционирования МССС по предоставлению услуг связи пользователям KF целесообразно построение сетей доступа, сетей агрегации и транспортных сетей, составляющих МССС, с использованием структур вида "звезда", линейных структур, кольцевых структур, древовидных стуктур и (или) их комбинации в соответствии с применимостью. Для достижения требуемых значений коэффициента готовности МССС КГi целесообразно построение i-ых подсетей, составляющих МССС, перечисленными ранее структурами с минимальным средним расстоянием, с минимальным диаметром, с требуемым средним коэффициентом связности узлов, с выровненной мощностью сечений сети [3], с использованием однородных графов Мура и (или) Синглтона (если возможно) [4], с использованием конечных абелевых изотропных симметричных структур [5], евклидовых решеток с замкнутыми границами [3] и (или) близких к таковым, построение минимального остовного дерева по вершинам, по ребрам и(или) их комбинации и пр. Для достижения требуемого значения интегрального показателя затрат всех ресурсов, необходимых для функционирования МССС Q целесообразно построение подсетей МССС с использованием существующих линейно-технических элементов сетевой инфраструктуры МССС как с учетом приведенных ранее структур, так и с применением автоматизированных алгоритмов, например, алгоритма "резиновой нити" поиска составных трасс и пр.

Следует отметить, что формулируемые выше частные способы и методы синтеза подсетей, составляющих МССС, обладают достаточно высокой взаимозависимостью. При этом, время, как основной показатель оперативности функционирования МССС, также прямо или опосредованно входит в каждый из интегральных показателей, приведенных в [1] а данные показатели имеют различный целевой экстремум. Все приведенные рассуждения в совокупности объективно обуславливают отсутствие строгих математических методов решения задачи синтеза МССС, поскольку, например, методы, приведенные в [3], также, в свою очередь, являются компромиссными и (или) подоптимальными и (или) околооптимальными решениями задачи синтеза МССС.

Таким образом, полученное предлагаемым методом решение обобщённой задачи структурно-параметрического синтеза МССС не будет являться строго оптимальным в соответствии с заданными в [1] критериями. Вместе с тем, можно утверждать, что найденное, в соответствии с формулируемыми подходом [1], способом (применение метода последовательных уступок) и предлагаемым методом решение будет принадлежать к области подоптимальных и (или) околооптимальных решений, поскольку учитывает ряд формализуемых и не формализуемых требований к функционированию МССС, а также может быть получено за приемлемое, например, по сравнению с методом полного перебора, время и с учётом величин выполняемых в ходе решения уступок и (или) получаемых за счет выполненных уступок выигрышей и (или) их соотношения.

СПИСОК ЛИТЕРАТУРЫ

1. Журавель Е.П. Постановка задачи синтеза структуры мультисервисной сети связи ограниченного пользования и способ ее решения // Информация и космос, 2015, №3. С. 40 - 48.
2. Подиновский В.В. Введение в теорию важности критериев в многокритериальных задачах принятия решений. - М.: ФИЗМАТЛИТ, 2007, 64 с.
3. Лебедев А.Т., Бабкин А.В., Муравцов А.А. Многокритериальный синтез топологической структуры региональной транспортной сети связи. // Научно-технический вестник Санкт-Петербургского государственного политехнического университета, 2008, № 3. С. 12 - 17.
4. Артамонов Г.Т., Тюрин В.Д. Топология сетей ЭВМ и многопроцессорных систем. - М.: Радио и связь, 1991, 248 с.
5. Евреинов Э.В, Хорошевский В.Г. Однородные вычислительные системы. - Новосибирск: Наука, 1978, 320 с.

ОГЛАВЛЕНИЕ

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В СФЕРЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 5

КВАЛИМЕТРИЧЕСКАЯ ПАРАДИГМА ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЩЕСТВА
Алексеев Анатолий Владимирович 5

ГОСУДАРСТВЕННЫЕ УСЛУГИ НА ПУТИ К ЦИФРОВИЗАЦИИ
Дединкина Евгения Олеговна 11

ПРЕДЛОЖЕНИЯ ПО СОЗДАНИЮ ТИПОВОЙ ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ СВЯЗИ ОПОРНОЙ ЗОНЫ РАЗВИТИЯ В АРКТИКЕ
Кулешов Игорь Александрович, Солозобов Сергей Анатольевич, Шевченко Василий Васильевич 14

ОСНОВНЫЕ НАПРАВЛЕНИЯ РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
Сторожик Виктор Сергеевич 18

ВОПРОСЫ ИНТЕРОПЕРАБЕЛЬНОСТИ ГОРОДСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ САНКТ-ПЕТЕРБУРГА
Шиян Артём Викторович, Митягин Сергей Александрович 25

ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ИНФОРМАТИКИ И ИНФОРМАТИЗАЦИИ 30

НЕКОТОРЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ РАДИОЧАСТОТНЫХ МЕТОК НА ПОВЕРХНОСТНЫХ АКУСТИЧЕСКИХ ВОЛНАХ
Верзун Наталья Аркадьевна, Колбанев Михаил Олегович, Омельян Александр Владимирович 30

КОГНИТИВНЫЕ ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ ДЛЯ МОНИТОРИНГА
Водяхо Александр Иванович, Осипов Василий Юрьевич, Червонцев Михаил Александрович, Жукова Наталия Александровна 33

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ЗОНДОВОГО ПРОТОКОЛА МАРШРУТИЗАЦИИ ДЛЯ MANET СЕТЕЙ В СРЕДЕ МАТЛАБ
Дорогов Александр Юрьевич 38

ОЦЕНКА ЭФФЕКТИВНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ
Зубаха Александр Максимович, Подружкина Татьяна Александровна, Саратов Дмитрий Николаевич, Редковников Владислав Александрович 43

КРИТЕРИИ И МЕТОДЫ ОЦЕНКИ КАЧЕСТВА ДЛЯ ОБОСНОВАНИЯ ВЫБОРА МЕЖСЕТЕВЫХ ЭКРАНОВ
Протас Роман Сергеевич, Закороев Расул Романович 48

АВТОМАТИЧЕСКИЙ РАЗЛИЧИТЕЛЬ ВЕТРОВОГО СЛИКА И НЕФТЯНОГО ПЯТНА
Чернецова Елена Анатольевна, Шишкин Анатолий Дмитриевич 51

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 54

КИБЕРБЕЗОПАСНОСТЬ ЦИФРОВОГО ПРОИЗВОДСТВА И ЭКОНОМИКИ
Зегжда Петр Дмитриевич 54

ЗАЩИТА ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ ОТ ПРОГРАММ-ВЫМОГАТЕЛЕЙ
Андреев Владислав Павлович, Черных Андрей Климентьевич 62

УГРОЗЫ ВЗЛОМА БЕСПРОВОДНЫХ СЕТЕЙ И МЕРЫ ПО ИХ ПРЕДОТВРАЩЕНИЮ
Андреев Владислав Павлович, Черных Андрей Климентьевич 65

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ЯЗЫКА RUBY И ФРЕЙМВОРКА RAILS И МЕТОДЫ ИХ РЕШЕНИЯ
Жарков Арсений Дмитриевич, Савков Сергей Витальевич, Садикова Анастасия Александровна 68

ПОСТКВАНТОВЫЙ АЛГОРИТМ ЦИФРОВОЙ ПОДПИСИ, ОСНОВАННЫЙ НА СКРЫТОЙ ЗАДАЧЕ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ
Молдовян Николай Андреевич, Абросимов Иван Константинович 71

КРИТЕРИИ И ПОКАЗАТЕЛИ КЛАССИФИКАЦИИ ИНСАЙДЕРОВ
Поляничко Марк Александрович, Королев Александр Игоревич 75

МЕТОДИКА ОПРЕДЕЛЕНИЯ НАДЕЖНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ
Садикова Анастасия Александровна, Кузнецов Александр Юрьевич, Жарков Арсений Дмитриевич 76

ИССЛЕДОВАНИЕ ФОРМИРОВАНИЯ БИПОЛЯРНЫХ СВЕРХКОРОТКИХ ИМПУЛЬСОВ НАПРЯЖЕНИЯ БОЛЬШОЙ МОЩНОСТИ НА ОСНОВЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ
Сорокин Леонид Николаевич, Усыченко Алексей Сергеевич 79

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ И ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... 84

ИСТОЧНИКИ УГРОЗ И ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ
Бобонец Сергей Алексеевич, Костюк Анатолий Владимирович..... 84

УГРОЗЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ
Костюк Анатолий Владимирович, Николаев Иван Андреевич..... 87

БЕЗОПАСНОСТЬ ПРИМЕНЕНИЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ ОРГАНАХ ВНУТРЕННИХ ДЕЛ
Локнов Алексей Игоревич, Примакин Алексей Иванович 90

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ МВД РОССИИ
Саратов Дмитрий Николаевич, Редковников Владислав Александрович 94

РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ ОРГАНИЗАЦИОННЫХ МЕРОПРИЯТИЙ И СОВЕРШЕНСТВОВАНИЮ ЗАКОНОДАТЕЛЬСТВА МВД В ОТНОШЕНИИ СОТРУДНИКОВ, ДОПУЩЕННЫХ К СВЕДЕНИЯМ, СОСТАВЛЯЮЩИМ ГОСУДАРСТВЕННУЮ ТАЙНУ
Чудаков Олег Евгеньевич, Попова Наталья Сергеевна, Иванов Даниил Дмитриевич 98

АСПЕКТЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ ЗАЩИТЫ ЛИЧНОСТИ
Ярмоленко Наталия Владимировна..... 102

КЛАСТЕРНЫЙ АНАЛИЗ КАК ИНСТРУМЕНТ ДЛЯ ОБРАБОТКИ ДАННЫХ ПСИХОЛОГИЧЕСКИХ ИССЛЕДОВАНИЙ
Ярмоленко Наталия Владимировна..... 104

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ 108

МАТЕМАТИКО-СТАТИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ УВЕЛИЧЕНИЯ ДОЛГА НАСЕЛЕНИЯ ПЕРЕД БАНКАМИ
Большакова Людмила Валентиновна, Смолина Яна Николаевна, Яковлева Наталья Александровна ... 108

АРХИТЕКТУРА ЦИФРОВОЙ ЭКОНОМИКИ
Верзун Наталья Аркадьевна, Колбанёв Михаил Олегович, Шамин Алексей Анатольевич..... 110

ВРЕМЕННАЯ ДИАГРАММА ПОТОКА СОБЫТИЙ КАК ИНСТРУМЕНТ ОЦЕНКИ ОПЕРАЦИОННОГО РИСКА ПРЕДПРИЯТИЯ
Карасева Екатерина Ивановна 114

ЭФФЕКТИВНОСТЬ УПРАВЛЕНЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
Лукьянова Людмила Михайловна..... 119

ОПЕРАТИВНАЯ АНАЛИТИЧЕСКАЯ ОБРАБОТКА ДАННЫХ МОНИТОРИНГА ОКУПАЕМОСТИ РЕАЛЬНЫХ ИНВЕСТИЦИЙ
Смирнова Елена Юрьевна 124

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ 128

ЦИФРОВИЗАЦИЯ ПРОЦЕССОВ ВЗАМОДЕЙСТВИЯ СИСТЕМ АВИАЦИОННОГО ТРАНСПОРТНО-ЛОГИСТИЧЕСКОГО УЗЛА
Зайцев Евгений Николаевич, Коникова Елена Викторовна..... 128

РАЗРАБОТКА И ПРИМЕНЕНИЕ ИМИТАЦИОННЫХ МОДЕЛЕЙ ПРИ УПРАВЛЕНИИ ПОТОКАМИ ПАССАЖИРОВ В АЭРОВОКЗАЛАХ
Зайцев Евгений Николаевич, Пашкевич Алексей Георгиевич, Тецлав Илья Александрович, Шайдуров Иван Георгиевич 131

ИСПОЛЬЗОВАНИЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ПЕРЕВОЗКЕ НЕГАБАРИТНЫХ ГРУЗОВ
Искандеров Юрий Марсович, Свистунова Александра Сергеевна, Чумак Александр Сергеевич..... 136

СИСТЕМА УПРАВЛЕНИЯ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ НА ОСНОВЕ НЕЙРОСЕТЕЙ: ЗАВИСИМОСТЬ РЕАЛИЗАЦИИ ОТ ТИПА РЕШАЕМЫХ ЗАДАЧ
Кудряшов Константин Витальевич, Балса Алдрин Раульевич 140

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ СИСТЕМ СКЛАДИРОВАНИЯ КОНТЕЙНЕРНЫХ ТЕРМИНАЛОВ
Николаевский Николай Николаевич, Козлова Дарья Викторовна 143

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ 150

УСЛОВИЯ ИНФОРМАТИЗАЦИИ ПЕРСПЕКТИВНЫХ СИСТЕМ ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ ПРАКТИЧЕСКОЙ ПОДГОТОВКОЙ
Алексеев Сергей Алексеевич, Парфенов Николай Петрович, Стахно Роман Евгеньевич, Яковлева Наталья Александровна 150

ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ ПРИ СОЗДАНИИ ДОКУМЕНТОВ С ИСПОЛЬЗОВАНИЕМ MS OFFICE
Домбровская Лариса Александровна, Гончар Артем Александрович, Яковлева Наталья Александровна 154

РАЗВИТИЕ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАМКАХ ДВИЖЕНИЯ WORLDSKILLS В ТЕХНИКУМЕ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Голубева Ольга Павловна 157

ОБ ОСОБЕННОСТЯХ МОДЕЛИ ОЦЕНКИ КАЧЕСТВА СИСТЕМЫ ЭЛЕКТРОННОГО ОБУЧЕНИЯ ПО ISO 9126
Журавлев Антон Евгеньевич 160

ТЕОРИЯ СИСТЕМНЫХ ИССЛЕДОВАНИЙ КАК ОСНОВА ФУНДАМЕНТАЛЬНОЙ ОБЩЕНАУЧНОЙ ПОДГОТОВКИ МОЛОДЫХ УЧЕНЫХ
Калинин Владимир Николаевич 164

АНАЛИЗ ПРИМЕНЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ «ГАЛАКТИКА ERP» В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ
Локнов Алексей Игоревич, Примакин Алексей Иванович 168

ИННОВАЦИОННЫЕ МЕТОДЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ
Парфенов Николай Петрович, Алексеев Сергей Алексеевич, Стахно Роман Евгеньевич, Яковлева Наталья Александровна 171

ИНФОРМАТИКА КАК ОСНОВА ФУНДАМЕНТАЛЬНОЙ ПОДГОТОВКИ РАЗРАБОТЧИКОВ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ
Советов Борис Яковлевич 174

ПРОБЛЕМЫ МЕТОДИКИ ПРЕПОДАВАНИЯ ИНФОРМАТИКИ В ШКОЛАХ ЛИНГВИСТИЧЕСКОГО ПРОФИЛЯ
Фёдоров Константин Павлович 176

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕДИЦИНЕ И ЗДРАВООХРАНЕНИИ 186

ОПРЕДЕЛЕНИЕ ТИПА ЛИЧНОСТНОЙ АКЦЕНТУАЦИИ В СИСТЕМЕ ВЗАИМООТНОШЕНИЙ «ВРАЧ-ПАЦИЕНТ» В ОНКОЛОГИИ
Бланк Михаил Аркадьевич, Бланк Ольга Алексеевна, Минкин Виктор Альбертович, Николаенко Яна Николаевна 186

КЛАСТЕРНЫЙ АНАЛИЗ СТОМАТОЛОГИЧЕСКИХ ДАННЫХ
Никонорова Маргарита Леонидовна 189

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В МЕДИЦИНЕ
Шугай Антон Андреевич 193

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ ОБЪЕКТАМИ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ 197

ПРИНЦИПЫ АВТОМАТИЗАЦИИ ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ ОБРАЗОВАТЕЛЬНЫМИ СИСТЕМАМИ ПО ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО УПРАВЛЕНИЮ ОБЪЕКТАМИ МОРСКОЙ ИНФРАСТРУКТУРЫ
Алексеев Сергей Алексеевич, Парфенов Николай Петрович, Стахно Роман Евгеньевич, Яковлева Наталья Александровна 197

МОНИТОРИНГ ОБЪЕКТОВ МОРСКОГО И РЕЧНОГО ТРАНСПОРТА С ПОМОЩЬЮ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Балса Алдрин Раульевич 202

АЛГОРИТМИЗАЦИЯ АВТОМАТИЧЕКОЙ СИСТЕМЫ ВИБРАЦИОННОЙ ДИАГНОСТИКИ СУДОВОГО РОТОРНОГО ОБОРУДОВАНИЯ
Баркова Наталия Александровна, Грищенко Дмитрий Вячеславович 204

ВОЗМОЖНОСТИ ВИБРАЦИОННОЙ ДИАГНОСТИКИ ГАЗОТУРБИННЫХ ДВИГАТЕЛЕЙ
Баркова Наталия Александровна, Грищенко Дмитрий Вячеславович 206

КВАЛИМЕТРИЧЕСКОЕ РАНЖИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА CRM, А ТАКЖЕ ЛУЧШИХ ПРАКТИК ИХ ОСВОЕНИЯ В ЖИЗНЕННОМ ЦИКЛЕ ОБЪЕКТА МОРСКОЙ ТЕХНИКИ ТИПА СУДОВАЯ РАДИОЛОКАЦИОННАЯ СТАНЦИЯ
Бекетова Екатерина Александровна 210

АВТОМАТИЗИРОВАННАЯ ОПТИМИЗАЦИЯ КОМПЛЕКТАЦИИ ГЕНЕРАТОРНЫМИ АГРЕГАТАМИ ЭЛЕКТРОСТАНЦИИ СПГ-ТАНКЕРА
Голубев Роман Олегович 213

КВАЛИМЕТРИЧЕСКОЕ РАНЖИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА MRP II ПРИ ПРОЕКТИРОВАНИИ «ОКЕАНИЧЕСКОЙ ТЕПЛОВОЙ ЭЛЕКТРОСТАНЦИИ»
Даулетьярова Назгуль Кайнаровна 218

ОБОСНОВАНИЕ ЦЕЛЕСООБРАЗНОСТИ И СПОСОБА ВВЕДЕНИЯ В ОЛВМ ЛОГИЧЕСКОЙ ОПЕРАЦИИ «ПРИОРИТЕТ»
Можаева Ирина Александровна, Поленин Владимир Иванович, Струков Александр Владимирович, Сущенков Дмитрий Андреевич 220

ОБЕСПЕЧЕНИЕ СЕТЕВОЙ ОТКАЗОУСТОЙЧИВОСТИ И БАЛАНСИРОВКИ НАГРУЗКИ В РАСПРЕДЕЛЕННЫХ КОРАБЕЛЬНЫХ СИСТЕМАХ УПРАВЛЕНИЯ
Носков Илья Игоревич 224

КВАЛИМЕТРИЧЕСКОЕ РАНЖИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА SCADA, А ТАКЖЕ ЛУЧШИХ ПРАКТИК ИХ ОСВОЕНИЯ В ЖИЗНЕННОМ ЦИКЛЕ ОБЪЕКТА МОРСКОЙ ИНФРАСТРУКТУРЫ ПО РАЗРАБОТКЕ АВТОМАТЕЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ
Рогозин Михаил Юрьевич 229

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ 232

ЭКОНОМИЧЕСКИЙ ПОДХОД ПРИ ОБЕСПЕЧЕНИИ СОХРАНЕНИЯ ПРАГМАТИЧЕСКОЙ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В ГРУППЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ
Ким Юлия Вячеславовна, Викснин Илья Игоревич 232

РАЗРАБОТКА МЕТОДА ОБНАРУЖЕНИЯ И КОРРЕКЦИИ ОШИБОК ДЛЯ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СЕТИ НА ОСНОВЕ БОЛЬШИХ ДАННЫХ
Леснова Елена Михайловна, Пестов Игорь Евгеньевич 236

МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ ГРУППЫ БЕСПИЛОТНЫХ ЛЕТАЮЩИХ АППАРАТОВ В СРЕДЕ СИМУЛЯЦИИ V-REP
Турсуков Никита Олегович, Мариненков Егор Денисович 240

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦИФРОВОГО ПРОИЗВОДСТВА
Усова Мария Андреевна 242

МОДЕЛЬ ПОЛИЦЕЙСКИХ УЧАСТКОВ С ЧАСТИЧНО ЦЕНТРАЛИЗОВАННЫМ УПРАВЛЕНИЕМ В МОБИЛЬНОЙ РОБОТОТЕХНИЧЕСКОЙ СИСТЕМЕ
Чупров Сергей Сергеевич, Викснин Илья Игоревич, Усова Мария Андреевна 245

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ 250

СОДЕРЖАТЕЛЬНАЯ И ФОРМАЛЬНАЯ ПОСТАНОВКА ЗАДАЧИ ПЛАНИРОВАНИЯ ТЕХНИЧЕСКОГО ПЕРЕВООРУЖЕНИЯ ПРОМЫШЛЕННОГО ОБЪЕКТА
Захаров Валерий Вячеславович 250

ПОСТРОЕНИЕ И АППРОКСИМАЦИЯ ОБЛАСТЕЙ ДОСТИЖИМОСТИ: ОБЗОР СУЩЕСТВУЮЩИХ РЕШЕНИЙ И ВЫБОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
Ушаков Виталий Анатольевич 253

МЕТОД СИНТЕЗА МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ
Журавель Евгений Павлович 257

ОГЛАВЛЕНИЕ 259

CONTENTS 263

CONTENTS

GOVERNMENT POLICY IN THE FIELD OF INFORMATIZATION AND INFORMATION SECURITY 5

QUALITATIVE PARADIGM MODEL AND THE DIGITAL TRANSFORMATION OF SOCIETY
Alekseev Anatoly 5

PUBLIC SERVICES ON THE WAY TO DIGITALIZATION
Dedinkina Evgenia 11

PROPOSALS FOR THE CREATION OF THE MODEL OF THE GEOGRAPHICALLYDISTRIBUTED TELECOMMUNICATION NETWORK SUPPORT ZONE DEVELOPMENT IN THE ARCTIC
Kuleshov Igor, Solozobov Sergey, Shevchenko Vasily 14

THE MAIN DIRECTIONS OF THE STATE POLICY IN THE FIELD OF SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION
Storozhik Victor 18

ISSUES OF URBAN INFORMATION SYSTEMS INTEROPERABILITY in ST. PETERSBURG
Shiyan Artem, Mityagin Sergey 25

THEORETICAL PROBLEMS OF INFORMATICS AND INFORMATIZATION 30

SOME ASPECTS OF THE USE OF RFID TAGS SURFACE ACOUSTIC WAVE
Verzun Natalia, Kolbanev Mikhail, Omelyan Alexander 30

COGNITIVE GIS MONITORING SYSTEMS
Vodyaho Alexander, Osipov Vasiliy, Chervontsev Mikhail, Zhukova Natalia 34

SIMULATION OF PROBE ROUTING PROTOCOL FOR WIRELESS NETWORKS IN THE ENVIRONMENT OF MATLAB
Dorogov Alexander 38

ASSESSMENT OF THE EFFECTIVENESS OF AUTOMATED CONTROL SYSTEMS
Zubaha Aleksandr, Podruzhkina Tatiana, Saratov Dmitriy, Redkovnikov Vladislav 43

CRITERIA AND METHODS OF ASSESSMENT OF QUALITY FOR JUSTIFICATION OF THE CHOICE OF FIREWALLS
Protas Roman, Zakoroev Rasul 48

AUTOMATIC DEFINITION OF WIND SLIC AND PETROLEUM SPOT
Chernetsova Elena, Shishkin Anatoly 51

INFORMATION SECURITY 54

CYBERSECURITY OF DIGITAL INDUSTY AND ECONOMY
Zegzhda Peter 54

PROTECTING PERSONAL COMPUTERS FROM EXTORTION PROGRAMS
Andreev Vladislav, Chernykh Andrei 62

THREATS OF WRAPPING OF WIRELESS NETWORKS AND MEASURES ON THEIR PREVENTION
Andreev Vladislav, Chernykh Andrei 65

RUBY LANGUAGE SECURITY PROBLEMS AND RAILS FRAMEWORK AND METHODS OF THEIR SOLUTION
Zharkov Arseny, Savkov Sergey, Sadikova Anastasia 69

POST-QUANTUM DIGITAL SIGNATIRE PROTOCOL BASED ON THE HIDDEN DISCRETE LOGARITHM PROBLEM
Moldovyan Nikolay, Abrosimov Ivan 71

CRITERIA AND INDICATORS FOR CLASSIFYING INSIDERS
Polyanichko Mark, Korolev Alexander 75

THE METHOD OF DETERMINING THE RELIABILITY OF INFORMATION PROTECTION IN AN AUTOMATED INFORMATION SYSTEM IN SECURED EXECUTION
Sadikova Anastasiia, Kuznetsov Aleksandr, Zharkov Arseniy 77

STUDY OF THE FORMATION OF BIPOLAR ULTRA-SHORT VOLTAGE PULSES OF HIGH POWER ON THE BASIS OF SIMULATION
Sorokin Leonid, Usychenko Aleksey 79

INFORMATION-PSYCHOLOGICAL AND LEGAL ASPECTS OF INFORMATIZATION AND INFORMATION SECURITY 84

SOURCES OF THREATS AND PECULIARITIES OF SECURITY INFORMATION SECURITY PERSONALITY
Bobonets Sergey, Kostyuk Anatoliy 84

THREATS OF INFORMATION-PSYCHOLOGICAL SECURITY OF PERSONALITY IN INFORMATION SOCIETY
Kostyuk Anatoliy, Nikolaev Ivan 87

SECURITY OF CLOUD TECHNOLOGIES IN THE ACTIVITIES OF INTERNAL AFFAIRS BODIES
Loknov Aleksey, Primakin Alexey 90

AUTOMATION OF INFORMATION RISKS MANAGEMENT IN INFORMATION NETWORKS OF MIA OF RUSSIA
Saratov Dmitriy, Redkovnikov Vladislav 94

RECOMMENDATIONS FOR THE CONDUCT OF ORGANIZATIONAL ACTIVITIES AND IMPROVING THE LEGISLATION OF THE MOI WITH REGARD TO THE EMPLOYEES APPROPRIATE TO THE STATE SECRET
Chudakov Oleg, Popova Natalia, Ivanov Daniil 99

ASPECTS OF INFORMATION-PSYCHOLOGICAL PROTECTION OF THE PERSON
Yarmolenko Natalia 102

CLUSTER ANALYSIS AS A TOOL FOR DATA PROCESSING PSYCHOLOGICAL RESEARCH
Yarmolenko Natalia 104

INFORMATION TECHNOLOGIES IN ECONOMY 108

MATHEMATICAL-STATISTICAL STUDY OF THE INCREASE OF THE POPULATION DEBT TO BANKS
Bolshakova Lyudmila, Smolina Jana, Yakovleva Natalia 108

ARCHITECTURE OF THE DIGITAL ECONOMY
Verzun Natalia, Kolbanev Mikhail, Shamin Alexey 110

TIME DIAGRAM OF EVENT FLOW AS A TOOL FOR OPERATIONAL RISK ESTIMATION IN ENTERPRISE
Karaseva Ekaterina 114

EFFICIENCY OF ACTIVITIES IN AUTOMATED INFORMATION SYSTEMS
Lukyanova Lyudmila 119

CAPITAL EXPENDITURES PROFITABILITY MONITORING DATA ONLINE ANALYTICAL PROCESSING
Smirnova Elena 125

INFORMATION TECHNOLOGIES IN TRANSPORT 128

DIGITAL FORM OF THE PROCESSES OF CO-OPERATION OF THE SYSTEMS OF AIR TRANSPORTATION LOGISTICS HUB
Zaitsev Evgeniy, Konikova Elena 128

DEVELOPMENT AND APPLICATION OF IMITATION MODELS AT CONTROL OF FLOWS IN PASSENGERS TERMINALS
Zaitsev Evgeniy, Pashkevich Aleksey, Teclav Ilya, Shaydurov Ivan 132

THE USE OF THE INTELLECTUAL DECISION SUPPORT SYSTEM FOR OVERSIZE CARGO TRANSPORTATION
Iskanderov Yury, Svistunova Alexandra, Chumak Alexander 137

CONTROL SYSTEM UNMANNED AERIAL VEHICLE ON THE BASIS OF NEURAL NETWORKS: THE DEPENDENCE OF THE IMPLEMENTATION ON THE TYPE OF TASKS
Kudryashov Konstantin, Balsa Aldrin 140

SIMULATION OF CONTAINER TERMINAL STORAGE SYSTEM
Nikolaevskiy Nikolay, Kozlova Daria 144

INFORMATION TECHNOLOGIES IN EDUCATION 150

THE CONDITIONS OF INFORMATIZATION OF PROMISING SYSTEMS OF ORGANIZATIONAL MANAGEMENT PRACTICAL TRAINING
Alekseev Sergey, Parfenov Nikolay, Sakhno Roman, Yakovleva Natalia 150

AUTOMATION TECHNOLOGIES FOR CREATING DOCUMENTS USING MS OFFICE
Dombrovskaya Larisa, Gonchar Artem, Yakovleva Natalia 154

INFORMATION TECHNOLOGY DEMO EXAM WORLDSKILLS THE COLLEGE OF RAILWAY TRANSPORT
Golubeva Olga..... 157

ABOUT FEATURES OF E-LEARNING SYSTEM QUALITY ASSESSING ACCORDING TO ISO 9126
Zhuravlev Anton 160

THE THEORY OF SYSTEM RESEARCHES AS A BASIS OF FUNDAMENTAL GENERAL SCIENTIFIC PREPARATION OF YOUNG SCIENTISTS
Kalinin Vladimir..... 164

ANALYSIS OF THE USE OF THE AUTOMATED CONTROL SYSTEM «GALAXY ERP» IN THE EDUCATIONAL PROCESS OF ST. PETERSBURG UNIVERSITY OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA
Loknov Aleksey, Primakin Alexey 168

INNOVATIVE METHODS OF TRAINING OF SPECIALISTS ON SAFETY OF INFORMATION TECHNOLOGIES IN THE LAW-ENFORCEMENT SPHERE
Parfyonov Nikolay, Alekseev Sergey, Stakhno Roman, Yakovleva Natalya 171

INFORMATICS AS BASIS OF FUNDAMENTAL TRAINING OF DEVELOPERS OF INFORMATION TECHNOLOGIES AND SYSTEMS
Sovetov Boris 174

THE PROBLEMS OF THE METHODICS OF TEACHING INFORMATICS AT SCHOOLS OF LINGUISTIC PROFILE
Fyodorov Konstantin 177

INFORMATION TECHNOLOGIES IN MEDICINE AND PUBLIC HEALTH 186

EXPRESS DIAGNOSTICS OF PERSONALITY ACCENTUATION TYPES. FIRST CLINICAL EXPERIENCE IN ONCOLOGY
Blank Mikhail, Blank Olga, Minkin Viktor, Nikolaenko Yana..... 186

CLUSTER ANALYSIS OF DENTAL DATA
Nikonorova Margarita 189

BLOCKCHAIN IN MEDICINE: USE CASES OF TECHNOLOGY
Shugai Anton 193

INFORMATION TECHNOLOGIES OF MANAGEMENT OF MARINE TECHNIQUE OBJECTS AND MARINE INFRASTRUCTURE 197

PRINCIPLES OF AUTOMATION IN ORGANIZATIONAL MANAGEMENT OF EDUCATIONAL SYSTEMS FOR TRAINING SPECIALISTS IN MANAGEMENT OF OBJECTS OF THE MARITIME INFRASTRUCTURE
Alekseev Sergey, Parfenov Nikolay, Sakhno Roman, Yakovleva Natalia 197

OBJECTS' MONITORING OF THE MARITIME AND INLAND TRANSPORT BY MEANS OF MODERN INFORMATION TECHNOLOGIES
Balsa Aldrin 202

ALGORITHMS FOR AUTOMATIC DIAGNOSTIC SYSTEMS WICH USE VIBRATION SIGNALS
Barkova Nataliya, Grishchenko Dmitriy..... 204

THE CAPABILITYES OF GAS-TURBINE DIAGNOSTICS BY VIBRATION SIGNAL
Barkova Nataliya, Grishchenko Dmitriy..... 207

KVALIMETRIC RANGE OF INFORMATION TECHNOLOGIES OF THE CLASS CRM, AND THE BEST PRACTICES OF THEIR DEVELOPMENT IN THE LIFE CYCLE OBJECTS OF MARINE TECHNOLOGY TYPE SHIP RADAR STATION
Beketova Ekaterina 211

SURVEY OF AUXILIARY GEN SET TYPES COMBINATIONS AUTOMATED OPTIMIZATION FOR LNG CARRIERS
Golubev Roman..... 213

QUALIMETRIC RANKING OF INFORMATION TECHNOLOGIES OF THE CLASS MRP II WHEN DESIGNING THE «OCEANIC HEAT ELECTRIC POWER STATION»
Dauletyarova Nazgul 218

JUSTIFICATION OF VALIDITY AND METHOD OF INTRODUCTION OF THE LOGIC OPERATION «PRIORITY»
Mozhaeva Irina, Polenin Vladimir, Strukov Alexander, Suuschenkov Dmitry 220

PROVIDING FAULT-TOLERANCE OF NETWORK AND LOAD BALANCING FOR DISTRIBUTED MARINE CONTROL SYSTEMS
Noskov Ilya 224

QUALITATIVE RANKING OF INFORMATION TECHNOLOGY CLASS SCADA, AS WELL AS THE BEST PRACTICES OF THEIR DEVELOPMENT IN THE LIFE CYCLE OF THE OBJECT OF MARITIME INFRASTRUCTURE DEVELOPMENT AUTOMATED CONTROL SYSTEM
Rogozin Mikhail 229

YOUTH SCIENTIFIC SCHOOL SAFE INFORMATION TECHNOLOGY 232

ECONOMIC APPROACH IN PROVIDING PRAGMATIC INFORMATION INTEGRITY PRESERVATION IN A GROUP OF UNMANNED AERIAL VEHICLES
Kim Iuliia, Viksnin Ilya 232

DEVELOPMENT OF THE METHOD OF DETECTION AND CORRECTION ERRORS FOR BIG DATA BASED DISTRIBUTED INFORMATION NETWORK
Lesnova Elena, Pestov Igor 236

MODEL OF FUNCTIONING OF THE PILOTLESS FLYING DEVICES IN THE ROBOT SIMULATION ENVIRONMENT V-REP
Tursukov Nikita, Marinenkov Egor 240

INFORMATION SECURITY THREATS OF DIGITAL MANUFACTURING
Usova Maria 242

POLICE OFFICE MODEL WITH PARTIALLY CENTRALIZED CONTROL IN MOBILE ROBOTIC SYSTEM
Chuprov Sergey, Viksnin Ilia, Usova-Maria 245

YOUTH SCIENTIFIC SCHOOL INFORMATION TECHNOLOGIES MATHEMATICAL MODELING 250

FORMAL AND NOTIONAL PROBLEM'S DESCRIPTION OF PLANNING AN INDUSTRIAL FACILITY'S TECHNICAL REEQUIPMENT
Zakharov Valerii 250

REACHABILITY AREA CONSTRUCTION AND APPROXIMATION: REVIEW EXISTING SOLUTIONS AND A CHOICE OF SOFTWARE
Ushakov Vitaly 254

METHOD OF SYNTHESIS OF A MULISERVICE COMMUNICATION NETWORK
Zhuravel Evgeny 257