ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2023)

XIII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 25-27 октября 2023 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург
2023

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2023)

XIII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 25-27 октября 2023 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург

2023

УДК (002:681):338.98

И 74

Информационная безопасность регионов России (ИБРР-2023).

И 74 XIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 25-27 октября 2023 г.: Материалы конференции / СПОИСУ. – СПб., 2023. – 401 с.

ISBN 978-5-00182-087-1

Сборник охватывает широкий круг направлений: Государственная политика обеспечения информационной безопасности регионов России; Правовые аспекты информационной безопасности; Безопасность информационных технологий; Информационная безопасность телекоммуникационных сетей; Информационно-экономическая безопасность; Информационная безопасность транспортных систем; Информационная безопасность объектов морской техники и морской инфраструктуры; Информационно-психологическая безопасность; Информационная безопасность в социокомпьютинге; Информационная безопасность киберфизических систем; Подготовка и переподготовка кадров в области обеспечения информационной безопасности, а также материалы круглого стола «Обеспечение информационной безопасности системы распределенных ситуационных центров» и молодежных научных школ «Экосистема безопасных городских цифровых сервисов», «Безопасные интеллектуальные информационные системы и технологии». Предназначен для широкого круга руководителей и специалистов органов государственной власти, академических учреждений, высших учебных заведений, научно-исследовательских и научно-производственных предприятий и организаций Санкт-Петербурга и других регионов, специализирующихся в области 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 11.10.2023. Формат 60x84⅛. Бумага офсетная.
Печать – ризография. Усл. печ. л. 46,6. Тираж 400 экз. Заказ № 1247
Отпечатано в ООО «ИПЦ «Измайловский»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-00182-087-1

© Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления (СПОИСУ), 2023 г.
© Авторы, 2023 г.

INFORMATION SECURITY OF RUSSIAN REGIONS (ISRR-2023)

XIII ST. PETERSBURG INTERREGIONAL CONFERENCE

St. Petersburg, October 25-27, 2023

PROCEEDINGS OF THE CONFERENCE

St. Petersburg

2023

УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ

- Правительство Санкт-Петербурга
- Законодательное Собрание Санкт-Петербурга
- Правительство Ленинградской области
- Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
- Министерство науки и высшего образования Российской Федерации
- Российская академия образования
- Отделение нанотехнологий и информационных технологий Российской академии наук
- Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
- Санкт-Петербургская территориальная группа Российского национального комитета по автоматическому управлению
- Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления

СОУСТРОИТЕЛИ КОНФЕРЕНЦИИ

- СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
- Военная академия связи им. С.М. Буденного
- ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н. Г. Кузнецова»
- Государственный университет морского и речного флота имени адмирала С.О. Макарова
- Российский государственный гидрометеорологический университет
- Санкт-Петербургский государственный морской технический университет
- Санкт-Петербургский государственный университет аэрокосмического приборостроения
- Санкт-Петербургский государственный университет телекоммуникаций им. профессор М.А. Бонч-Бруевича
- Санкт-Петербургский государственный экономический университет
- Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
- Санкт-Петербургский институт экономики и бизнеса
- Санкт-Петербургский научный центр Российской академии наук
- Санкт-Петербургский политехнический университет Петра Великого
- Санкт-Петербургский университет МВД России
- Университет ИТМО
- Группа компаний «Марвел»
- АО «Институт инфотелекоммуникаций»
- АО «Концерн «НПО «Аврора»
- АО «Научно-исследовательский институт программных средств»
- АО «Научно-производственное объединение «Импульс»
- АО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
- АО «НИИ «Масштаб»
- АО «Центр компьютерных разработок»
- ЗАО «Институт телекоммуникаций»
- ООО «Ассоциация специалистов безопасности»
- ООО «Геонавигатор»
- ООО «Лаборатория инфокоммуникационных сетей»
- ООО «НеоБИТ»
- ПАО «ИНТЕЛТЕХ»
- Партнерство для развития информационного общества на Северо-Западе России
- Санкт-Петербургская инженерная академия
- Санкт-Петербургское отделение Академии инженерных наук им. А.М. Прохорова
- Санкт-Петербургское отделение Академии информатизации образования
- Санкт-Петербургское отделение Международной академии информатизации

Конференция организована в рамках цикла мероприятий «ИТ-Диалог 2023»

КООРДИНАЦИОННЫЙ СОВЕТ КОНФЕРЕНЦИИ

Беглов Александр Дмитриевич	Губернатор Санкт-Петербурга
Бельский Александр Николаевич	Председатель Законодательного собрания Санкт-Петербурга
Дрозденко Александр Юрьевич	Губернатор Ленинградской области
Фальков Валерий Николаевич	Министр науки и высшего образования Российской Федерации
Шадаев Максут Игоревич	Министр цифрового развития, связи и массовых коммуникаций Российской Федерации
Красников Геннадий Яковлевич	Президент Российской академии наук, академик Российской академии наук
Шакин Дмитрий Николаевич	Руководитель Управления Федеральной службы технического и экспортного контроля по Северо-Западному федеральному округу
Шерстюк Владислав Петрович	Президент Национальной ассоциации международной информационной безопасности, член-корреспондент Академии криптографии Российской Федерации, советник Секретаря Совета Безопасности Российской Федерации

ПРЕЗИДИУМ КОНФЕРЕНЦИИ

Советов Борис Яковлевич	Председатель Президиума конференции, председатель Программного комитета, сопредседатель Научного совета по информатизации Санкт-Петербурга, академик Российской академии образования
Юсупов Рафаэль Мидхатович	Председатель Организационного комитета, научный руководитель СПИИРАН – СПб ФИЦ РАН, член-корреспондент Российской академии наук
Белов Евгений Борисович	Председатель Федерального УМО ВО в области информационной безопасности, заместитель начальника института криптографии, связи и информатики «Академии ФСБ России»
Ильин Николай Иванович	Заместитель начальника Управления информационных систем Службы специальной связи и информации ФСО России
Казарин Станислав Валериевич	Вице-губернатор Санкт-Петербурга
Максимов Андрей Станиславович	Председатель Комитета по науке и высшей школе Санкт-Петербурга
Панкевич Виктор Николаевич	Первый заместитель начальника управления делами Администрации Губернатора Санкт-Петербурга
Пешехонов Владимир Григорьевич	Научный руководитель ГНЦ «Центральный научно-исследовательский институт «Электроприбор», академик Российской академии наук
Ронжин Андрей Леонидович	Директор Санкт-Петербургского Федерального исследовательского центра Российской академии наук, профессор РАН
Смирнова Юлия Леонидовна	Председатель Комитета по информатизации и связи Санкт-Петербурга
Смирнов Анатолий Иванович	Генеральный директор Национальной ассоциации международной информационной безопасности, профессор Московского государственного института международных отношений (университета) Министерства иностранных дел Российской Федерации, председатель Отделения РАЕН «Информационная глобализация»
Стрельцов Анатолий Александрович	Вице-президент Национальной ассоциации международной информационной безопасности, профессор, ведущий научный сотрудник факультета вычислительной математики Московского государственного университета им. М.В. Ломоносова, действительный государственный советник Российской Федерации 3 класса

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Председатель Организационного Комитета

Юсупов Рафаэль Мидхатович	Научный руководитель СПИИРАН – СПб ФИЦ РАН, член-корреспондент Российской академии наук

Заместитель председателя Организационного Комитета

Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций», президент Санкт-Петербургского отделения Академии информатизации образования, председатель Экспертного совета Санкт-Петербургского информационно-аналитического центра

Члены Организационного Комитета

Алексеев Анатолий Владимирович	Исполнительный директор Института автоматизации процессов борьбы за живучесть корабля, судна, профессор кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета
Антохина Юлия Анатольевна	Ректор Санкт-Петербургского государственного университета аэрокосмического приборостроения
Барышников Сергей Олегович	Ректор Государственного университета морского и речного флота имени адмирала С.О. Макарова
Басков Вячеслав Дмитриевич	Генеральный директор ООО «НеоБИТ»
Блажис Анатолий Константинович	Директор АО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
Бобрович Владимир Юрьевич	Директор по стратегическому и инновационному развитию АО «Концерн «НПО «Аврора»
Богданов Владимир Николаевич	Директор АО «ЦентрИнформ», лауреат Государственной премии Российской Федерации в области науки и техники
Борисов Николай Валентинович	Заведующий кафедрой Санкт-Петербургского государственного университета
Васильев Владимир Николаевич	Ректор Университета ИТМО, член-корреспондент Российской академии образования, член-корреспондент Российской академии наук
Гаценко Олег Юрьевич	Генеральный директор АО «Научно-исследовательский институт программных средств»
Гирдин Сергей Алексеевич	Президент Группы компаний «Марвел»
Григорьев Владимир Александрович	Генеральный директор ООО «Лаборатория инфокоммуникационных сетей», президент Санкт-Петербургского отделения Общероссийской общественной организации «Академия инженерных наук им. А.М. Прохорова»
Демидов Алексей Вячеславович	Ректор Санкт-Петербургского государственного университета промышленных технологий и дизайна, вице-президент Российского союза ректоров, председатель Совета ректоров вузов Санкт-Петербурга и Ленинградской области
Жданов Сергей Николаевич	Советник генерального директора АО ВТБ Девелопмент по внешним связям
Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций», президент Санкт-Петербургского отделения Академии информатизации образования, председатель Экспертного совета Санкт-Петербургского информационно-аналитического центра
Зайцева Александра Алексеевна	Ученый секретарь СПб ФИЦ РАН
Захаров Юрий Никитич	Первый заместитель директора СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Зегжда Дмитрий Петрович	Директор Института кибербезопасности и защиты информации Санкт-Петербургского политехнического университета Петра Великого, член-корреспондент РАН

Ипатов Олег Сергеевич	Начальник управления научно-технологического партнерства Санкт-Петербургского политехнического университета Петра Великого
Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, заместитель начальника отдела аспирантуры СПб ФИЦ РАН
Кефели Игорь Федорович	Ведущий научный сотрудник лаборатории стратегического планирования и евразийской интеграции Северо-Западного института управления - филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации
Корниенко Анатолий Адамович	Профессор кафедры информатики и информационной безопасности Петербургского государственного университета путей сообщения Императора Александра I
Крупцов Сергей Владимирович	Первый заместитель генерального директора АО «Центр компьютерных разработок»
Кузичкин Александр Васильевич	Главный научный сотрудник АО «НИИ телевидения»
Кузьмин Юрий Григорьевич	Ученый секретарь Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Кулешов Игорь Александрович	Заместитель генерального директора по научной работе ПАО «ИНТЕЛТЕХ»
Куприянов Михаил Степанович	Руководитель научного и образовательного направлений, заведующий кафедрой вычислительной техники Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
Кучерявый Михаил Михайлович	Советник генерального директора АО «Корпорация Московский институт теплотехники» Государственной корпорации «Роскосмос», Государственный советник Российской Федерации 1 класса
Максименко Андрей Владимирович	Директор СПб ГУП «Санкт-Петербургский информационно-аналитический центр», координатор федерального проекта «Цифровая Россия» по Санкт-Петербургу
Максимцев Игорь Анатольевич	Ректор Санкт-Петербургского государственного экономического университета
Минаев Николай Николаевич	Первый заместитель директора СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Михайлов Николай Семенович	Заместитель генерального директора по информационным технологиям и стратегии развития АО «Равенство»
Михайлова Анна Сергеевна	Заместитель директора Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления по связям с общественностью
Михеев Валерий Леонидович	Ректор Российского государственного гидрометеорологического университета
Молдовян Александр Андреевич	Главный научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем СПИИРАН – СПб ФИЦ РАН
Николашин Юрий Львович	Генеральный директор ПАО «ИНТЕЛТЕХ», генеральный конструктор системы управления ВМФ
Никулин Евгений Николаевич	Ректор Санкт-Петербургского института экономики и бизнеса
Ныркov Анатолий Павлович	И.о. заведующего кафедрой комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова
Оводенко Анатолий Аркадьевич	Президент Санкт-Петербургского государственного университета аэрокосмического приборостроения
Присяжнюк Сергей Прокофьевич	Генеральный директор ЗАО «Институт телекоммуникаций»
Пролетарский Андрей Викторович	Декан Московского государственного технического университета им. Н.Э. Баумана, председатель Федерального УМО по УГСН 09.00.00 «Информатика и вычислительная техника»

Пухов Геннадий Георгиевич	Директор ООО «Геонавигатор»
Силла Евгений Петрович	Ученый секретарь СПИИРАН – СПб ФИЦ РАН
Смирнов Павел Игоревич	Генеральный директор АО «НИИ «Масштаб»
Солодянников Александр Владимирович	Генеральный директор ООО «Ассоциация специалистов безопасности»
Строганов Дмитрий Викторович	Профессора кафедры АСУ Московского автомобильно-дорожного государственного технического университета (МАДИ), эксперт РАН, председатель Учебно-методического совета 09.00.02 «Информационные системы и технологии»
Тихомиров Сергей Григорьевич	Генеральный директор АО «Центр компьютерных разработок»
Туричин Глеб Андреевич	Ректор Санкт-Петербургского государственного морского технического университета
Черешкин Дмитрий Семенович	Заведующий лабораторией Института системного анализа Федерального исследовательского центра «Информатика и управление» Российской академии наук
Чугунов Андрей Владимирович	Чугунов Андрей Владимирович, директор Центра технологий электронного правительства Института дизайна и урбанистики Университета ИТМО, генеральный директор НП ПРИОР Северо-Запад
Шелудько Виктор Николаевич	Ректор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
Шерстюк Юрий Михайлович	Генеральный директор АО «Институт инфотелекоммуникаций»
Шилов Константин Юрьевич	Генеральный директор АО «Концерн «НПО «Аврора»

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Председатель Программного Комитета

Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга, заслуженный профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), академик Российской академии образования, засл. деятель науки и техники РФ, д-р техн. наук, профессор

Заместители председателя Программного Комитета

Никонов Игорь Александрович	Первый заместитель председателя Комитета по информатизации и связи Санкт-Петербурга, канд. техн. наук

Члены программного комитета – руководители и секретари секций

Абрамов Максим Викторович	Руководитель лаборатории теоретических и междисциплинарных проблем информатики СПИИРАН – СПб ФИЦ РАН, канд. техн. наук
Алексеев Анатолий Владимирович	Исполнительный директор НП «Институт автоматизации процессов борьбы за живучесть корабля, судна», профессор кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, д-р техн. наук, профессор
Беззатеев Сергей Валентинович	Заведующий кафедрой информационной безопасности Санкт-Петербургского государственного университета аэрокосмического приборостроения, профессор факультета безопасности информационных технологий Университета ИТМО, д-р техн. наук, доцент
Бобрович Владимир Юрьевич	Директор по стратегическому и инновационному развитию АО «Концерн «НПО «Аврора», д-р техн. наук, профессор
Верзун Наталья Аркадьевна	Доцент кафедры информационных систем и технологий Санкт-Петербургского государственного экономического университета, канд. техн. наук, доцент
Виноградов Александр Андреевич	Главный эксперт АО «НПО «Импульс»

Воробьев Евгений Германович	Заведующий кафедрой информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), д-р техн. наук, доцент
Гадаев Егор Михайлович	Эксперт НП «Институт автоматизации процессов борьбы за живучесть корабля, судна»
Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций», президент Санкт-Петербургского отделения Академии информатизации образования, председатель Экспертного совета Санкт-Петербургского информационно-аналитического центра, д-р техн. наук, доцент
Заколдаев Данил Анатольевич	Декан факультета безопасности информационных технологий Университета ИТМО, канд. техн. наук, доцент
Зикратов Игорь Алексеевич	Декан факультета информационных систем и технологий, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, д-р техн. наук, профессор
Игумнов Владимир Вячеславович	Советник генерального директора АО «НПО «Импульс», профессор Академии военных наук, канд. техн. наук
Искандеров Юрий Марсович	Заведующий лабораторией информационных технологий на транспорте СПИИРАН – СПб ФИЦ РАН, д-р техн. наук, профессор
Истомин Евгений Петрович	Заведующий кафедрой прикладной информатики Российского государственного гидрометеорологического университета, д-р техн. наук, профессор
Кефели Игорь Федорович	Ведущий научный сотрудник лаборатории стратегического планирования и евразийской интеграции Северо-Западного института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, засл. работник высшей школы Российской Федерации, д-р филос. наук, профессор
Колбанёв Михаил Олегович	Профессор Санкт-Петербургского государственного экономического университета, д-р техн. наук, профессор
Коршунов Игорь Львович	Заведующий кафедрой информационных систем и технологий Санкт-Петербургского государственного экономического университета, канд. техн. наук, доцент
Котенко Игорь Витальевич	Главный научный сотрудник, руководитель лаборатории проблем компьютерной безопасности СПИИРАН – СПб ФИЦ РАН, д-р техн. наук, профессор, засл. деятель науки РФ
Коржук Виктория Михайловна	Доцент факультета безопасности информационных технологий Университета ИТМО, канд. техн. наук
Коротков Виталий Валерьевич	Доцент кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, канд. техн. наук, доцент
Ласкин Михаил Борисович	Старший научный сотрудник лаборатории интеллектуальных систем СПИИРАН – СПб ФИЦ РАН, канд. физ.-мат. наук, доцент
Левшун Дмитрий Сергеевич	Старший научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН – СПб ФИЦ РАН, канд. техн. наук
Литвинов Владислав Леонидович	Доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. профессор М.А. Бонч-Бруевича, канд. техн. наук, доцент
Локнов Алексей Игоревич	Майор полиции, доцент кафедры специальных информационных технологий Санкт-Петербургского университета МВД России, канд. техн. наук
Мельник Галина Сергеевна	Профессор кафедры цифровых медиакоммуникаций Высшей школы журналистики и массовых коммуникаций Санкт-Петербургского государственного университета, д-р полит. наук, профессор
Метелева Алина Сергеевна	Информационный менеджер Центра технологий электронного правительства Института дизайна и урбанистики Университета ИТМО, магистрант Института дизайна и урбанистики Университета ИТМО

Микадзе Сергей Юрьевич	Проректор Санкт-Петербургского государственного экономического университета, канд. экон. наук
Михайличенко Антон Валерьевич	Адъюнкт Военной академии связи им. С.М. Буденного
Михальчук Андрей Васильевич	Доцент кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, канд. техн. наук
Мороз Николай Васильевич	Заместитель директора ООО «Геонавигатор»
Мусатенко Роман Иванович	Руководитель Центра ранговой партнерской сертификации НП «Институт автоматизации процессов борьбы за живучесть корабля, судна», старший научный сотрудник ВУНЦ ВМФ «ВМА»
Ныркov Анатолий Павлович	И.о. заведующего кафедрой комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, д-р техн. наук, профессор
Паращук Игорь Борисович	Профессор кафедры автоматизированных систем специального назначения Военной академии связи им. С.М. Буденного, д-р техн. наук, профессор, засл. изобретатель РФ
Петренко Сергей Анатольевич	Профессор кафедры информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), д-р техн. наук, профессор
Плебанек Ольга Васильевна	Заведующая кафедрой социально-гуманитарных дисциплин Университета при МПА ЕврАзЭС, д-р филос. наук, доцент
Примакин Алексей Иванович	Полковник полиции, начальник кафедры специальных информационных технологий Санкт-Петербургского университета МВД России, д-р техн. наук, профессор
Пухов Геннадий Георгиевич	Директор ООО «Геонавигатор», канд. техн. наук, профессор
Саенко Игорь Борисович	Ведущий научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН – СПб ФИЦ РАН, д-р техн. наук, профессор
Свешникова Наталья Олеговна	Доцент кафедры политической психологии факультета психологии Санкт-Петербургского государственного университета, канд. психол. наук, доцент
Согонов Сергей Александрович	Заведующий кафедрой судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, канд. техн. наук, доцент
Соколов Борис Владимирович	Заведующий лабораторией информационных технологий в системном анализе и моделировании, главный научный сотрудник СПИИРАН – СПб ФИЦ РАН, засл. деятель науки России, д-р техн. наук, профессор
Соколов Сергей Сергеевич	Проректор Российского университета транспорта, профессор кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, д-р техн. наук, доцент
Устинов Игорь Анатольевич	Советник генерального директора АО «Научно-производственное объединение «Импульс», канд. техн. наук, член-корреспондент Академии военных наук
Татарникова Татьяна Михайловна	Директор института информационных технологий и программирования Санкт-Петербургского государственного университета аэрокосмического приборостроения, д-р техн. наук, профессор
Филатова Ольга Георгиевна	Доцент кафедры связей с общественностью в политике и государственном управлении Санкт-Петербургского государственного университета, ведущий научный сотрудник Центра технологий электронного правительства Института дизайна и урбанистики Университета ИТМО, канд. филос. наук, доцент
Хлобыстова Анастасия Олеговна	Младший научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики СПИИРАН – СПб ФИЦ РАН
Цехановский Владислав Владимирович	Заведующий кафедрой информационных систем, Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук, доцент

Чугунов Андрей Владимирович	Чугунов Андрей Владимирович, директор Центра технологий электронного правительства Института дизайна и урбанистики Университета ИТМО, генеральный директор НП ПРИОР Северо-Запад, канд. политич. наук, доцент
Юсупов Рафаэль Мидхатович	Научный руководитель СПИИРАН – СПб ФИЦ РАН, член-корреспондент Российской академии наук, засл. деятель науки и техники РФ, д-р техн. наук, профессор
Яковлева Наталья Александровна	Полковник полиции, начальник кафедры математики и информатики Санкт-Петербургского университета МВД России, канд. психол. наук

Ученый секретарь Конференции

Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, заместитель начальника отдела аспирантуры СПб ФИЦ РАН, канд. техн. наук, доцент

ОБЩАЯ ПРОГРАММА РАБОТЫ КОНФЕРЕНЦИИ

ДЕНЬ ПЕРВЫЙ

25 октября 2023, среда

ОТКРЫТИЕ КОНФЕРЕНЦИИ, ПЕРВОЕ ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Место проведения: Дом ученых им. М. Горького,
Адрес: Санкт-Петербург, Дворцовая наб., д. 26, Белый зал
Проезд: ст. метро «Гостиный двор» или «Невский проспект», выход на канал Грибоедова

9:00 Регистрация гостей и участников Конференции «ИБРР-2023»
10:00 Торжественное открытие Конференции «ИБРР-2023»

ПРЕДСТАВЛЕНИЕ ОРГАНИЗАТОРОВ, УЧАСТНИКОВ И ГОСТЕЙ КОНФЕРЕНЦИИ

Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга, академик Российской академии образования

ПРИВЕТСТВИЯ ГОСТЯМ И УЧАСТНИКАМ КОНФЕРЕНЦИИ

Казарин Станислав Валериевич	Вице-губернатор Санкт-Петербурга
Шакин Дмитрий Николаевич	Руководитель Управления Федеральной службы технического и экспортного контроля по Северо-Западному федеральному округу

ПЛЕНАРНЫЕ ДОКЛАДЫ

14:00 Обед
15:00 Продолжение пленарного заседания

ДЕНЬ ВТОРОЙ

26 октября 2023, четверг

СЕКЦИОННЫЕ ЗАСЕДАНИЯ

Место проведения: по секциям

10:00 Секционные заседания
14:00 Обед
15:00 Секционные заседания

ДЕНЬ ТРЕТИЙ

27 октября 2023, пятница

СЕКЦИОННЫЕ ЗАСЕДАНИЯ

Место проведения: по секциям

10:00 Секционные заседания
14:00 Обед

ЗАКЛЮЧИТЕЛЬНОЕ ПЛЕНАРНОЕ ЗАСЕДАНИЕ

27 октября 2023 г., пятница, 15:00–18:00

Место проведения: Дом ученых им. М. Горького
Адрес: Санкт-Петербург, Дворцовая наб., д. 26, Белый зал
Проезд: ст. метро «Гостиный двор» или «Невский проспект», выход на канал Грибоедова

14:00 Регистрация участников заключительного пленарного заседания Конференции

ПЛЕНАРНЫЕ ДОКЛАДЫ

ОТЧЕТЫ РУКОВОДИТЕЛЕЙ СЕКЦИЙ КОНФЕРЕНЦИИ, ПРИНЯТИЕ РЕЗОЛЮЦИИ КОНФЕРЕНЦИИ

18:00 Закрытие Конференции. Отъезд гостей и участников Конференции

ПЛЕНАРНЫЕ ДОКЛАДЫ

1. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ САНКТ-ПЕТЕРБУРГА

Казарин Станислав Валериевич	Вице-губернатор Санкт-Петербурга,
Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга, академик Российской академии образования

2. СТРАТЕГИЯ РАЗВИТИЯ СЕТИ МНОГОФУНКЦИОНАЛЬНЫХ ЦЕНТРОВ В САНКТ-ПЕТЕРБУРГЕ

Смирнова Юлия Леонидовна	Председатель Комитета по информатизации и связи,
Александров Максим Михайлович	Директор СПб ГКУ «Многофункциональный центр предоставления государственных и муниципальных услуг»

3. МЕТОДОЛОГИЯ И ТЕХНОЛОГИИ ПРОАКТИВНОГО УПРАВЛЕНИЯ МОДЕРНИЗАЦИЕЙ КАТАСТРОФОУСТОЙЧИВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Охтилев Михаил Юрьевич	Генеральный директор АО «НИО ЦИТ «ПЕТРОКОМЕТА»,
Соколов Борис Владимирович	Заведующий лабораторией информационных технологий в системном анализе и моделировании, главный научный сотрудник СПИИРАН – СПб ФИЦ РАН
Юсупов Рафаэль Мидхатович	Научный руководитель СПИИРАН – СПб ФИЦ РАН, член-корреспондент Российской академии наук

4. ПЕРСПЕКТИВЫ РАЗВИТИЯ ЦЕНТРОВ УПРАВЛЕНИЯ РЕГИОНАМИ

Ильин Николай Иванович	Заместитель начальника Управления информационных систем Службы специальной связи и информации ФСО России,
Пухов Геннадий Георгиевич	Директор ООО «Геонавигатор»

5. БЕЗОПАСНОСТЬ БОЛЬШИХ ДАННЫХ

Зегжда Дмитрий Петрович	Директор Института компьютерных наук и кибербезопасности Санкт-Петербургского политехнического университета Петра Великого, член-корреспондент РАН,
Полтавцева Мария Анатольевна	Профессор Высшей школы кибербезопасности Института компьютерных наук и кибербезопасности Санкт-Петербургского политехнического университета Петра Великого

6. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ КИБЕРБЕЗОПАСНОСТИ: КЛЮЧЕВЫЕ НАПРАВЛЕНИЯ НАУЧНЫХ ИССЛЕДОВАНИЙ

Котенко Игорь Витальевич	Главный научный сотрудник, руководитель лаборатории проблем компьютерной безопасности СПИИРАН – СПб ФИЦ РАН

7. КРИЗИС ПРАВА В ЦИФРОВУЮ ЭПОХУ И СОЗДАНИЕ ИНФОРМАЦИОННОГО (ЦИФРОВОГО) КОДЕКСА

Наумов Виктор Борисович	Главный научный сотрудник лаборатории прикладной информатики и проблем информатизации общества СПб ФИЦ РАН, главный научный сотрудник Сектора информационного права и международной информационной безопасности Института государства и права РАН, профессор кафедры информационного права и цифровых технологий МГЮА, управляющий партнер офиса в Санкт-Петербурге юридической фирмы Nextons

8. КИБЕРБЕЗОПАСНОСТЬ И СМЕЖНЫЕ ПОНЯТИЯ. НАУЧНО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ В УСЛОВИЯХ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций», президент Санкт-Петербургского отделения Академии информатизации образования, председатель Экспертного совета Санкт-Петербургского информационно-аналитического центра

9. НАУЧНО-ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ КОГНИТИВНОЙ БЕЗОПАСНОСТИ

Кефели Игорь Федорович	Ведущий научный сотрудник лаборатории стратегического планирования и евразийской интеграции Северо-Западного института управления - филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации

10. РАЗРАБОТКА ПОСТКВАНТОВЫХ КРИПТОАЛГОРИТМОВ С ОТКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ КОНЕЧНЫХ АЛГЕБР

Молдовян Николай Андреевич	Главный научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем СПИИРАН – СПб ФИЦ РАН, профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)

11. ОСНОВЫ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ПО ОБНАРУЖЕНИЮ, ПРЕДУПРЕЖДЕНИЮ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Сторожик Виктор Сергеевич	Ведущий специалист Арктического и антарктического научно-исследовательского института

12. СВОБОДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И БЕЗОПАСНОСТЬ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Карпов Роман Дмитриевич	Директор по стратегии и развитию технологий Axiom JDK, советник Министра цифрового развития, связи и массовых коммуникаций РФ по вопросам системного ПО, руководитель комитета по информационной безопасности АРПП «Отечественный софт»

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ

УДК 004.8:336.1

ОЦЕНКА РИСКОВ ПРИ РЕГИОНАЛЬНОМ УПРАВЛЕНИИ

Булдакова Татьяна Ивановна, Джалолов Ахмад Шарофиддинович
Московский государственный технический университет им. Н.Э. Баумана
2-я Бауманская ул., 5, Москва, 105005, Россия
e-mails: buldakova@bmstu.ru, dzhalolov@mail.ru

Аннотация. Рассматриваются особенности регионального управления. Отмечена необходимость обеспечения информационной безопасности путем управления информационными рисками. Предложен подход для оценки рисков при бюджетном кредитовании регионов.

Ключевые слова: социально-экономическое состояние региона; информационные процессы; информационная безопасность; информационные риски; риски бюджетного кредитования.

RISK ASSESSMENT IN REGIONAL MANAGEMENT

Buldakova Tatiana, Dzhalolov Ahmad
Bauman Moscow State Technical University
2nd Baumanskaya St., 5, Moscow, 105005, Russia
e-mails: buldakova@bmstu.ru, dzhalolov@mail.ru

Abstract. The features of regional management are considered. The necessity of ensuring information security by managing information risks is noted. An approach for risk assessment in budget lending to regions is proposed.

Keywords: socio-economic state of the region; information processes; information security; information risks; risks of budget lending.

Оценка различных рисков (информационных, возникновения нежелательных процессов в регионе и других) является важной задачей при региональном управлении. Управление рисками подразумевает оценку их уровня и выработку контрмер для снижения или исключения негативных факторов. Для повышения эффективности регионального управления и исключения возможных рисков важным является объективная оценка социально-экономического состояния региона [1].

Реализация информационных процессов при региональном управлении требует интеграции и обработки разнотипной информации, а также защиты анализируемых данных и разработки концепции региональной информационной безопасности [2, 3]. Информационные процессы для оценки социально-экономического состояния региона оказываются уязвимыми к внешним (несанкционированным) воздействиям на информацию, которые могут носить и целенаправленный характер, что обусловливает необходимость постоянного отслеживания уровня информационных рисков. Таким образом, при региональном управлении необходимо решать проблему информационной безопасности, в том числе путем управления рисками ИБ. Для управления рисками информационной безопасности требуется применять множество методов, используемых на различных этапах процесса оценки уровня рисков и удовлетворяющих соответствующим показателям эффективности: 1) наибольшая согласованность и адекватность оценок факторов риска; 2) максимальная адаптивность к качественным данным; 3) минимальная субъективность и неопределённость оценки риска; 4) учёт неодинаковой чувствительности риска к различным факторам [4]. Пример решения задачи управления информационными рисками при обеспечении ИБ региональных информационных процессов приведен в работе [5].

Важной задачей, связанной с развитием региона, является принятие решения о предоставлении ему бюджетного кредита. Данное решение основывается на оценке социально-экономической ситуации в регионе, на основе которой требуется оценить риск невозврата бюджетных средств, поскольку минимизация такого риска является главным условием предоставления региону бюджетного кредита. Поэтому в основе решения задачи о бюджетном кредитовании регионов лежит анализ показателей их социально-экономического развития, который необходимо провести для определения возможности возврата бюджетных средств. Для принятия решения требуется учесть множество разнородных показателей, которые поступают из различных источников, имеют разное происхождение и степень влияния на принятие положительного или отрицательного решения.

Программный модуль, реализующий оценку социально-экономического состояния регионов, повышает объективность оценки рисков в процессе принятия решений по бюджетному кредитованию [6].

СПИСОК ЛИТЕРАТУРЫ

1. Булдакова Т.И., Джалолов А.Ш. Управление развитием регионов на основе анализа рейтингов региональных процессов // Инжиниринг предприятий и управление знаниями: сборник научных трудов XXIV Международной научной конференции. Москва: РЭУ им. Г. В. Плеханова, 2022. С. 16-22.
2. Булдакова Т.И., Джалолов А.Ш. Анализ информационных процессов и выбор технологий обработки и защиты данных в ситуационных центрах // Научно-техническая информация. Серия 1. 2012. № 6. С. 16-22.
3. Советов Б.Я., Касаткин В.В. Идеология построения концепции региональной информационной безопасности // Перспективные направления развития отечественных информационных технологий – Севастополь: ФГАОУ ВО «Севастопольский государственный университет», 2021. С. 46-50.
4. Булдакова Т.И., Миков Д.А. Обеспечение согласованности и адекватности оценки факторов информационного риска // Вопросы кибербезопасности. 2017. №3 (21). С. 8-15.
5. Булдакова Т.И., Джалолов А.Ш. Особенности разработки интеллектуальной системы защиты информации в ситуационном центре // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2014. № 4. С. 1-8.
6. Dzhalolov A.S., Buldakova T.I., Proletarsky A. Socio-Economic Decision Support Module by Unstructured Data. // Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg and Moscow, Russia, 2020, pp. 1931-1934. DOI: 10.1109/EIConRus49466.2020.9039086.

УДК 378.14

КИБЕРБЕЗОПАСНОСТЬ И СМЕЖНЫЕ ПОНЯТИЯ. НАУЧНО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ В УСЛОВИЯХ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Жигадло Валентин Эдуардович
ЗАО «Институт телекоммуникаций»,
Кантемировская ул., 5, лит. М, Санкт-Петербург, 194100, Россия
e-mail: zve@mail.ru

Аннотация. В докладе рассматриваются основы методологии информационной безопасности, её особенности, формируемые в условиях резкого обострения противоборства в современном информационном пространстве, новые задачи и функции информационной безопасности в условиях информационного противоборства и «ментальных» войн, обосновывается значимость и задачи информационно-психологической и когнитивной безопасности. Проводится анализ стратегии национальной безопасности Российской Федерации и других нормативных актов в части вопросов информационной безопасности. Особое внимание уделяется вопросу роли и месту в структуре информационной безопасности такого нового аспекта безопасности в информационной сфере, как кибербезопасность. Проводится детальный анализ стратегий кибербезопасности наиболее активных на мировой арене государств, ориентированных на проведении не только оборонительных, но и наступательных операций в киберпространстве, рассматриваются цели создания ведомств, ответственных за кибероперации.

Ключевые слова: информационныетехнологии, информационная безопасность, защита информации, защита от информации, информационный суверенитет, информационный потенциал, кибербезопасность, киберпространство, кибероперации.

CYBERSECURITY AND RELATED CONCEPTS. SCIENTIFIC AND METHODOLOGICAL ASPECTS IN THE CONDITIONS OF MODERN INFORMATION WARFARE

Zhigadlo Valentin
ZAO «Institute of Telecommunications»,
5 Kantemirovskaya str., lit. M, St. Petersburg, 194100, Russia
e-mail: zve@mail.ru

Abstract. The report examines the basics of the methodology of information security, its features formed in the conditions of a sharp escalation of confrontation in the modern information space, new tasks and functions of information security in the conditions of information confrontation and «mental» wars, substantiates the importance and tasks of information psychological and cognitive security. The analysis of the national security strategy of the Russian Federation and other regulations in terms of information security issues is carried out. Particular attention is paid to the role and place in the structure of information security of such a new aspect of security in the information sphere as cybersecurity. A detailed analysis of cybersecurity strategies of the most active states on the world stage, focused on conducting not only defensive, but also offensive operations in cyberspace, is carried out, the goals of creating departments responsible for cyber operations are considered.

Keywords: information technologies, information security, information protection, information protection, information sovereignty, information potential, cybersecurity, cyberspace, cyber operations.

В настоящее время, в условиях усиливающегося информационного противоборства, против России развернута и ведется необъявленная информационная война, направленная на уничтожение самосознания, изменение ментальной (цивилизационной) основы нашего государства, получившая название «ментальной» войны [1]. Поэтому несомненным приоритетом и значимостью обладает задача разработки

концепции информационной безопасности, определяющей принципы построения и структуру региональной системы ИБ, официальные взгляды на цели, задачи, принципы и основные направления которой изложены в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646 [2] и принятой в 2021 году Стратегии национальной безопасности Российской Федерации [3].

В докладе подробно рассматриваются методологические основы ИБ, определяющие двойственный характера воздействия информации на человека и социальную среду, новые задачи защиты от деструктивного, разрушительного воздействия информации. Отмечается важность развития и формирования в недрах теории информационной безопасности новой ее междисциплинарной составляющей — информационно-психологической и когнитивной безопасности (ИПКБ). Подробно анализируются механизмы реализации функций ИБ, обеспечивающие формирование государственного суверенитета в информационном пространстве на региональном уровне. Рассматривается структура потенциалов страны, развитие которых обеспечит формирование устойчивого иммунитета против деструктивного информационного воздействия и, как следствие, укрепление государственного суверенитета в региональном информационном пространстве. Особое внимание уделяется вопросам подготовки кадров в области ИБ. Проводится ретроспективный анализ мероприятий по нормализации вопросов в области ИБ, проведённых в стране за последний период.

Обращается внимание на то, что в последние десятилетия, особенно с принятием рядом наиболее активных на мировой арене государств стратегий кибербезопасности, ориентированных на проведении не только оборонительных, но и наступательных операций в киберпространстве и предполагающих создание ведомств, ответственных за кибероперации, кибер-терминология стала целенаправленно внедряться в некоторые научные тексты, чему трудно назвать иные причины, кроме потребности как-то дифференцировать технические аспекты в широком контексте вопросов информационной безопасности, особенно в условиях интенсивного развития информационных технологий и технологий искусственного интеллекта.

Так, например, в сборниках трудов Института системного анализа РАН «Проблемы кибербезопасности информационного общества» [4], авторам рекомендовалось при описании технологических аспектов использовать вместо прилагательного «информационные» приставки «кибер-», и, как следствие, соответственно, возникали «киберсистемы», «кибертехнологии», «киберпроцессы», «киберобъекты», киберкомпоненты», «киберриски» и т. п.

В этой связи, в целях определения роли и места кибербезопасности в предметной области информационной безопасности, в докладе проводится детальный анализ принятых за последние десятилетия у нас в стране нормативных стратегических и доктринальных документов в области информационной безопасности [2-3], а также, принятых в разных зарубежных странах (США, Великобритания, ФРГ, Королевство Испания, Франция, Эстонская республика, Канада, Австралия, Япония, КНР, Украина, альянс НАТО, ЕС) государственных и национальных стратегий кибербезопасности [5].

Приводится анализ нормативных документов стран разработчиков стратегий кибербезопасности, цели стратегий кибербезопасности рассмотренных стран, используемый понятийный аппарат. Показано, что из 20 стратегических целей, сформулированных Агентством ENISA, наибольшее количество целей поставила перед собой Эстония (17), наименьшее — Германия (9), несмотря на самый объемный из рассмотренных документов, Испания поставила перед собой 15 целей, а Франция — 13.

Показано так же, что стратегия кибербезопасности Европейского Союза выглядит флагманским документом, который задает курс для стратегий стран-участниц союза, в которой говорится о четвертой промышленной революции (Индустрии 4.0), цифровом переходе, безопасности критической инфраструктуры и персональных данных своих граждан, о безопасности Интернета вещей и защите «европейских ценностей», также речь идет о цифровом суверенитете.

Практически во всех стратегиях утверждается, что дезинформация и пропаганда извне разрушительно влияет на население.

По результатам проведенного анализа в докладе делается вывод о том, что если предметная область кибербезопасности и имеет право на самостоятельная существование, то только как составная часть предметной области информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Ильницкий А. М. Безопасность страны как фундамент развития. М. : Арсенал Отечества, 2021. № 1 (51).
2. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646.
3. Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 02.07.2021 г. № 400.
4. Проблемы кибербезопасности информационного общества // Труды Института системного анализа Российской академии наук. Т. 27. М. : КомКнига, 2006. 208 с.
5. Экспертно-аналитический центр группы компаний InfoWatch. Аналитический отчёт: «Стратегии Кибербезопасности», 2022. [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/strategii-kiberbezopasnosti-1.pdf (дата обращения: 30.09.2023).

УДК 004.413

СВОБОДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И БЕЗОПАСНОСТЬ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Карпов Роман Дмитриевич
ООО «БЕЛЛСОФТ»
Обводного канала наб., 199-201, литер Ж, 90020, Санкт-Петербург, 190020, Россия
e-mail: roman.karpov@axiomjdk.ru

Аннотация. Обсуждаются особенности применения свободного программного обеспечения с учетом требований импортозамещения. Анализируются риски неконтролируемого применения свободного программного обеспечения в государственных информационных системах и на объектах критической информационной инфраструктуры. Рассматриваются линейка продуктов и решения JDK Pro как доверенного отечественного поставщика программного обеспечения с открытым кодом для разработки и запуска Java приложений.

Ключевые слова: свободное программное обеспечение, государственные информационные системы, объекты критической информационной инфраструктуры, риски неконтролируемого применения свободного программного обеспечения, импортозамещение и информационная безопасность, линейка продуктов JDK Pro.

FREE SOFTWARE AND SECURITY OF STATE INFORMATION SYSTEMS AND CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

Karpov Roman Dmitrievich
BELLSOFT LLC
199-201 Obvodny Canal emb., letter Zh, 90020, St. Petersburg, 190020, Russia
e-mail: roman.karpov@axiomjdk.ru

Abstract. The differences between free and open source software are examined, and the features of using free software are discussed taking into account the requirements of import substitution. The risks of uncontrolled use of free software in government information systems and critical information infrastructure facilities are analyzed. The JDK Pro product and solution line is considered as a trusted domestic open source software provider for developing and running Java applications.

Keywords: free software, government information systems, critical information infrastructure facilities, risks of uncontrolled use of free software, import substitution and information security, JDK Pro product line.

Свободное или открытое программное обеспечение (ПО) — неотъемлемая часть современного ИТ-ландшафта: оно стимулирует инновации и быстрое развитие технологий и упрощает процесс разработки. Кроме того, учитывая современные реалии, свободное ПО становится решением многих проблем, связанных с импортозамещением. В частности, разработчики могут собрать стек из российских компонентов взамен иностранным решениям, да еще и совершенно бесплатно [1]. Но так ли все просто на самом деле?

Особенности применения свободного ПО с учетом требований импортозамещения

В соответствии со стандартом ГОСТ Р 54593-2011, свободное ПО (СПО) — это ПО, которое распространяется на условиях простой (неисключительной) лицензии, оставляющей за лицензиаром права выдачи лицензий другим лицам. Существует также термин «открытое программное обеспечение». Открытое ПО распространяется на условиях открытой лицензии (лицензионный договор, по которому простая лицензия предоставляется в упрощенном порядке и соответствует требованиям ст. 1286.1 Гражданского кодекса РФ).

Разница между свободным и открытым ПО определяется условиями лицензии, по которой данное ПО распространяется. Существует множество открытых и свободных лицензий, самые популярные из которых — MIT, Apache, GPL. Проект OpenJDK, имплементация языка программирования Java, разрабатывается под свободной лицензией GPLv2 with Classpath Exception (с исключением классов): это значит, что разработчики в своем приложении могут сочетать как открытые библиотеки, так и собственные наработки, и код последних открывать не нужно.

Открытое и свободное ПО отличаются друг от друга в зависимости от применяемой лицензии, но часто эти термины используются как синонимы. ПО с открытым кодом не всегда находится в открытом доступе, заказчик получает доступ к исходному коду после оформления подписки.

Далее мы будем использовать термин «свободное ПО» (СПО) в качестве обобщающего понятия для этих трех явлений.

На принципах свободного ПО построены многие решения, в том числе ОС Linux, браузер Mozilla Firefox, СУБД PostgreSQL и многие другие. Объем СПО, используемого в корпоративном стеке, может достигать 90%, и что самое главное — компоненты СПО могут использоваться в государственных системах, хотя и с важными оговорками.

Применение СПО в государственных ИТ-системах и на объектах КИИ

В соответствии с Указами Президента РФ №166 и №250 государственным и системообразующим предприятиям, субъектам КИИ и ГИС запрещено использовать иностранное ПО с января 2025 года.

Согласно Приказу Минцифры № 21 от 18 января 2023 г., утверждены методические рекомендации по переходу на использование российского ПО, в том числе для ГИС и на объектах КИИ.

В информационных системах органов государственной власти и на объектах КИИ разрешено использовать только ПО, входящие в Единый реестр российского ПО или Единый реестр евразийского ПО. ПО, относящиеся к СПО, также должны быть включены в реестры. В случае, если ПО не включено ни в один из реестров, оно по умолчанию относится к иностранному ПО, использование которого не допускается.

Соответственно, компания может использовать СПО в любом объеме при условии, что все компоненты зарегистрированы в реестрах.

Мы рекомендуем тщательно отслеживать происхождение всех компонентов, используемых в корпоративной разработке. Если в реестрах пока нет комплексного решения, полностью замещающего иностранный продукт, можно собрать комбинацию из нескольких компонентов от разных разработчиков. Реестры ПО постоянно пополняются, поэтому формирование стека утвержденных технологий в скором времени не составит труда.

Риски неконтролируемого применения свободного ПО

Допустим, ИТ-специалисты компании нашли в реестрах все необходимое ПО, которое к тому же является свободным, а значит, находится в открытом доступе. Значит ли это, что теперь можно совершенно бесплатно собрать корпоративный стек безопасных и производительных технологий?

На этот вопрос можно сформулировать два ответа:

– Разработчики бесплатно собирают стек технологий;

– Разработчики собирают стек безопасных и производительных технологий.

Почему так?

Дело в том, что исходный код ПО и бинарный файл — это не одно и то же, и в разнице между двумя файлами кроются потенциальные риски безопасности.

Исходный код, как уже было сказано выше — это понятный для разработчика текст программы, составленный на каком-либо языке программирования. Исходный код находится в свободном доступе или предоставляется пользователям после скачивания ПО. Но исходный код невозможно запустить на компьютере напрямую, его сначала нужно компилировать в бинарный файл, содержащий двоичное представление машинных инструкций для конкретного процессора. На компиляцию уходит много времени — минуты, часы, в отдельных случаях даже сутки. При этом сборка отнимает значительную часть или даже все вычислительные ресурсы компьютера, которому к тому же необходимо иметь большое количество свободной оперативной памяти и места на жёстком диске. Наконец, нужно полностью воспроизвести среду сборки и уметь пользоваться сборочными системами, а для разных технологий и языков программирования они могут быть разными. Как следствие, сборка исходного кода повышает затраты на персонал и инфраструктуру и увеличивает срок вывода продукта на рынок.

Во избежание подобных неудобств в сообществе СПО принято в дополнение к исходным кодам предоставлять и собранные бинарные файлы, например, в виде публичных репозиториев для ОС или коллекции образов на Docker Hub. Но если вы скачиваете бинарный файл из публичных репозиториев, никто не гарантирует соответствие бинарного файла исходному коду. Он может содержать вредоносное ПО или уязвимости, добавленные случайно или намеренно, но ответственность за последствия внедрения такого кода в корпоративный стек ложится на ИТ-команду компании, а не на разработчиков, выложивших код в свободный доступ. Использование готовых бинарных файлов — это вопрос доверия, и для серьезного бизнеса, и в особенности субъектов КИИ поиск надежных доверенных партнеров становится приоритетным вопросом, от которого зависит критическая часть процессов разработки и эксплуатации ГИС и КИИ [2].

Конечно, можно проводить верификацию бинарных файлов самостоятельно, используя:

– Бинарный анализ, с помощью которого проверяется безопасность бинарного файла без учета исходного кода;

– Пентесты (тестирование на проникновение) — методы оценки безопасности путем моделирования атаки злоумышленников;

– Сканеры безопасности, анализирующие файл на наличие известных (находящихся в базах данных сканеров) уязвимостей.

Все эти мероприятия требуют значительных временных и финансовых ресурсов, а также внутренней ИТ-экспертизы, но при этом ни один из методов не поможет установить соответствие бинарного файла исходному коду. Также можно, имея на руках бинарный файл и исходный код, воссоздать сборочную среду, в ней скомпилировать исходный код в исполняемый файл и затем сравнить полученные результаты с изначальным бинарным файлом. Данная методика требует еще больших временных и ресурсных энергозатрат, но на выходе результаты могут отличаться от ожидаемых из-за влияния множества переменных при воссоздании сборочной среды. К тому же, как мы выяснили выше, для сборки исходного кода требуется мощное оборудование и много времени.

Существует еще один вариант — проведение дорогостоящих проверок бинарных файлов с помощью утилит, предоставляемых вендорами решений по безопасности. Однако для использования этих технологий все равно придется строить собственную инфраструктуру и нанимать узкоспециализированных инженеров.

«Но если тесты показали отсутствие проблем безопасности, зачем нужно дополнительно подтверждать соответствие бинарного файла исходному файлу?» Ответ прост: отсутствие подтвержденного соответствия исходному коду всегда оставляет брешь в информационной безопасности.

Учитывая все вышесказанное, вы готовы собирать зависимости из исходного кода или пропускать каждый компонент через десятки тестов безопасности, повторяя процесс при каждом обновлении ПО?

Как обезопасить ИТ-инфраструктуру с помощью доверенных продуктов

Эксплуатация и контроль безопасности СПО требуют существенных ресурсных затрат, эти издержки можно оптимизировать, разделив ответственность и приобретя лицензию у доверенного отечественного поставщика ПО с открытым кодом. В этом случае проверку соответствия бинарных файлов исходному коду осуществляет сам поставщик и предоставляет заказчикам простые инструменты для итогового контроля (например, checksum). Кроме того, поставщик проводит тщательное тестирование сборок перед каждым релизом и предоставляет круглосуточную техподдержку.

В области Java разработки таким поставщиком выступает команда Axiom JDK, которая разрабатывает и поддерживает среду исполнения Java Axiom JDK Pro, сервер приложений Libercat и ряд других утилит. Все продукты входят в Единый реестр российского ПО и совместимы с российскими ОС, СУБД-оборудованием и облаками.

ПО линейки Axiom JDK сочетают в себе преимущества открытого ПО и функционала, локализованного под российский рынок:

– исходный код продуктов не находится в свободном доступе, а предоставляется клиентам после оформления подписки;

– технологии разрабатываются в соответствии с концепцией жизненного цикла безопасной разработки SDL (Secure Development Lifecycle) и перед каждым релизом проходят через жесткий контроль качества, включающий структурный, статический, динамический анализы, регрессионное и PoC-тестирование и другие испытания;

– поскольку в корпоративной разработке невозможно обойтись без сторонних компонентов, инженеры Axiom JDK создали доверенный репозиторий самых востребованных Java библиотек с исходными кодами, проверенными на предмет закладок и вредоносного ПО. Объем верифицированного кода составляет 4 Гб, и репозиторий постоянно пополняется;

– среда исполнения Axiom JDK Certified сертифицирована ФСТЭК по 4 УД, что позволяет использовать ее на объектах КИИ и ГИС, где требуется сертификация информационных систем по ФСТЭК.

– инженеры с 25-летним опытом развития Java и OpenJDK оказывают техническую поддержку 24/7 и выпускают экстренные патчи безопасности и фиксы;

– Axiom JDK Pro поставляется с готовыми конфигурациями TLS-сертификатов Минцифры, и является допустимой средой функционирования КриптоПРО JCP и КриптоПРО CSP.

СПИСОК ЛИТЕРАТУРЫ

1. Почему Open Source — это не бесплатно [Электронный ресурс]. URL: https://axiomjdk.ru/announcements/2023/06/09/pochemu-open-source-eto-ne-besplatno/ (Дата обращения: 29. 09. 2023).
2. Импортозамещение ПО для критической информационной инфраструктуры [Электронный ресурс]. URL:https://axiomjdk.ru/announcements/2023/05/19/kii/ (Дата обращения: 29. 09. 2023).
3. Информационная безопасность в финансовой сфере с точки зрения законодательства [Электронный ресурс]. URL: https://axiomjdk.ru/announcements/2023/04/13/informatsionnaja-bezopasnost-v-finansovoj-sfere-s-tochki-zrenija-zakonodatelstva/ (Дата обращения: 29. 09. 2023).

УДК 519.8

МЕТОДОЛОГИЯ И ТЕХНОЛОГИИ ПРОАКТИВНОГО УПРАВЛЕНИЯ МОДЕРНИЗАЦИЕЙ КАТАСТРОФОУСТОЙЧИВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

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

[1] Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, лит. А, Санкт-Петербург, Россия, 190000

[2]СПИИРАН – СПб ФИЦ РАН
14-ая линия В.О., 39, Санкт-Петербург, Россия, 199178

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

Аннотация. В докладе предлагаются разработанные авторами научные основы формального описания и решения проблемы модернизации информационных систем (ИС) для обеспечения их катастрофоустойчивости. При этом формальное описание и исследование данной проблемы предлагается осуществлять в рамках более общей научной проблемы многокритериального структурно-функционального синтеза как самих ИС, так и комплексных программ их создания и модернизации в динамически изменяющихся условиях. Приводятся примеры решения ряда практических задач создания и использования указанных информационных систем для различных предметных областей.

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

METHODOLOGY AND TECHNOLOGIES FOR PROACTIVE MANAGEMENT AND CONTROL FOR MODERNIZATION OF DISASTER-TOLERANCE INFORMATION SYSTEMS

Okhtilev Mikhail[1], Sokolov Boris[2], Yusupov Rafael[2]

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

[2]SPIIRAS – SPCRAS
39 14th line, St. Petersburg, Russia, 199178

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

Abstracts. The report proposes the scientific foundations developed by the authors for a formal description and solution to the problem of modernizing information systems (IS) to ensure their disaster tolerant. At the same time, a formal description and study of this problem is proposed to be carried out within the framework of a more general scientific problem of multi-criteria structural and functional synthesis of both the information systems themselves and complex programs for their creation and modernization in dynamically changing conditions. Examples are given of solving a number of practical problems of creating and using these information systems for various subject areas.

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

Анализ существующих и прогнозируемых кризисных и чрезвычайных ситуаций, повсеместно возникающих в настоящее время в различных предметных областях, показывает, что они перестают быть отраслевыми, а перерастают в аварии и катастрофы, имеющие уже межотраслевой характер. В этих условиях проблемы повышения катастрофоустойчивости как бизнес-процессов, так информационной системы (ИС), обеспечивающей их выполнение, становятся весьма актуальными. При этом под катастрофоустойчивостью ИС в докладе понимается способность распределенного компьютерного комплекса, состоящего из нескольких систем, сохранять (восстанавливать) критически важные данные (информацию) и продолжать выполнять свои основные функции после массового (возможно, целенаправленного) уничтожения его компонентов в результате различных катаклизмов как природного характера, так и инспирированных человеком. ИС, обладающие такой способностью (свойством), будем называть катастрофоустойчивыми ИС (КАИС). Как правило, большинство существующих ИС не обладают требуемым уровнем катастрофоустойчивости, поэтому их необходимо постоянно модернизировать. Известно, что переход от «старого» (существующего) варианта ИС (старой КАИС) к «новому» (модернизированному) варианту не может быть проведён мгновенно. Это на практике приводит к тому, что на достаточно длительном интервале времени (периоде модернизации ИС (СКАИС)) происходит совместная эксплуатация элементов и подсистем «старой» и «новой» ИС (СКАИС). Однако, в этих условиях, показатели качества и эффективности бизнес-процессов, определяемые их предназначением и поддерживаемые (оптимизируемые) ИС (СКАИС), не должны ухудшаться. Таким образом, всякое изменение и развитие (модернизация) той или иной подсистемы (структуры) ИС (СКАИС) объективно осуществляется одновременно с решением оперативных (текущих) задач, стоящих перед соответствующей бизнес (целевой)-системой (БС, ЦС)). Поэтому возникает необходимость совместной постановки и решении следующих пяти задач комплексного планирования и управления модернизацией и функционированием ИС (КАИС). Необходимо сформировать (синтезировать) конечный облик соответствующей модернизируемой ИС (КАИС) (решить задачу структурно-функционального синтеза), определить сроки, к которым должна завершится указанная модернизация, определить технологии модернизации ИС (КАИС) (в рамках которой на каком-то интервале времени будут одновременно функционировать элементы и подсистемы «старой» и «новой» КАИС, чтобы обеспечить устойчивость функционирования соответствующих целевых (бизнес) процессов), определить программу перехода от «старой» и «новой» КАИС, и наконец сформировать программы перепланирования, либо коррекции исходной программы модернизации КАИС, если появятся непредусмотренные возмущающие воздействия. определить сроки, к которым должна завершится указанная модернизация, определить технологии модернизации ИС (СКАИС) (в рамках которой на каком-то интервале времени будут одновременно функционировать элементы и подсистемы «старой» и «новой» КАИС, чтобы обеспечить устойчивость функционирования соответствующих целевых (бизнес) процессов), определить программу перехода от «старой» и «новой» КАИС, и наконец сформировать программы перепланирования, либо коррекции исходной программы модернизации КАИС, если появятся непредусмотренные возмущающие воздействия [1-4].

Проведенные исследования показали, что рассматриваемые задачи целесообразно формально описывать и решать в рамках междисциплинарного подхода, интерпретируя их как задачи проактивного управления структурной динамикой (ПУСД) рассматриваемыми процессами и системами [5-6].

Предлагаемые в докладе методологические основы решения рассматриваемой проблемы модернизации КАИС базируются на четырех базовых концепциях, к числу которых отнесены концепции комплексного моделирования и проактивного управления, концепция инвариантности реальных и вычислительных процессов, их описывающих, а также концепция интеллектуализации процессов формирования и реализации управленческих процессов [7-8].

Для решения исследуемой проблемы модернизации Ис (КАИС), а также конструктивной реализации на практике перечисленных концепций в СПИИРАН были разработали две новые прикладные теории: теория проактивного управления жизненным циклом (ЖЦ) сложных объектов (СлО) и соответствующими АСУ, в которых данные управления реализуются, а также теорию многокритериального оценивания и выбора наиболее предпочтительных моделей и полимодельных комплексов (ПМК), описывающих процессы функционирования СлО и соответствующих АСУ на различных этапах их ЖЦ (квалиметрией моделей и ПМК). Последняя из перечисленных теорий, а именно, прикладная теория многокритериального оценивания качества моделей и полимодельных комплексов для решения задач проактивного управления ЖЦ СлО, обеспечивает детализацию и уточнение положений, развитых в общей квалиметрии моделей и полимодельных комплексов [7-9]. В докладе предложена оригинальная обобщенная методика решения задач комплексного планирования модернизации и функционирования КАИС в условиях динамично изменяющейся обстановки, которая включает две основные фазы.

На первой фазе должно осуществляться формирование (генерирование) допустимых вариантов многоструктурных макросостояний КАИС или, говоря другими словами, оперативный структурно-функциональный синтез нового облика ИС (КАИС), соответствующего целям проводимой модернизации и складывающейся (прогнозируемой) обстановке, связанной с возможной деградацией структур, создаваемой и существующей КАИС.

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

В докладе приводятся примеры практической реализации полученных научных результатов при создании и применении КАИС в различных предметных областях [9].

Исследование выполнено за счет гранта Российского научного фонда № 22-19-00767.

СПИСОК ЛИТЕРАТУРЫ

1. Кульга К. С. Особенности внедрения на предприятиях и методы интеграции CAD/CAM/PDM/FRP/MRP/MES/PLM и ERP-систем // САПР и графика. 2008. № 3. С. 91–94.
2. Будзко В. И. Количественные оценки отказоустойчивых и катастрофоустойчивых решений // Вопросы защиты информации. 2003. № 2. С. 19–32.
3. Управление жизненным циклом продукции / А. Ф. Колчин [и др.]. М. : Анахарсис, 2002. 304 с.
4. IC PLM10 // BIBA [Электронный ресурс]. URL: http://www.plm10.org (дата доступа: 01.10.2023).
5. Охтилев М. Ю., Мустафин Н. Г., Миллер В. Е., Соколов Б. В. Теоретические основы проактивного управления сложными объектами // Известия ВУЗОВ. Приборостроение. 2014. Т. 57. № 11. С. 7-15.
6. Охтилев М. Ю., Соколов Б. В. Юсупов Р. М., Стыскин М. М., Джао В. Ю-Д. Концепция и технологии проактивного управления жизненным циклом изделий // Известия высших учебных заведений. Приборостроение. 2020. Т. 63. № 2. С. 158-163.
7. Охтилев М. Ю., Соколов Б. В., Юсупов Р. М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. М. : Наука, 2006. 410 с.
8. Микони С. В., Соколов Б. В., Юсупов Р. М. Квалиметрия моделей и полимодельных комплексов. М. : РАН, 2018. 314 с.
9. ЛИТСАМ. Лаборатория информационных технологий в системном анализе и моделировании : [сайт]. URL: http:// litsam.ru (дата доступа: 01.10.2023).

УДК 004.056

ОСНОВЫ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ПО ОБНАРУЖЕНИЮ, ПРЕДУПРЕЖДЕНИЮ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕАГИРОВАНИЮ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

Сторожик Виктор Сергеевич
Арктический и антарктический научно-исследовательский институт
Беринга ул., 38, Санкт-Петербург, 199397, Россия
e-mail: vsstorozhik@aari.ru

Аннотация. Рассматривается нормативно-правовое обеспечение создания, функционирования и современного этапа развития государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Ключевые слова: защищенность, информационный ресурс, концепция, компьютерная атака, компьютерный инцидент, критическая информационная инфраструктура, обнаружение, предупреждение, реагирование, силы, средства, угроза, уязвимость.

FUNDAMENTALS OF STATE POLICY ON DETECTING, PREVENTING AND ELIMINATING THE CONSEQUENCES OF COMPUTER ATTACKS ON THE INFORMATION RESOURCES OF THE RUSSIAN FEDERATION AND RESPONDING TO COMPUTER INCIDENTS

Storozhik Viktor
Arctic and Antarctic Research Institute
38 Bering St., St. Petersburg, 199397, Russia
e-mail: vsstorozhik@aari.ru

Abstract. The article considers the regulatory and legal support for the creation, functioning and current stage of development of the state system for detecting, preventing and eliminating the consequences of computer attacks on the information resources of the Russian Federation.

Keywords: security, information resource, concept, computer attack, computer incident, critical information infrastructure, detection, warning, response, forces, means, threat, vulnerability.

В Доктрине информационной безопасности Российской Федерации состояние информационной безопасности (ИБ) в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак (КА) на объекты критической информационной инфраструктуры (КИИ) [1].

Стратегия национальной безопасности Российской Федерации указывает, что увеличивается количество КА на российские информационные ресурсы (ИР). Большая часть таких атак осуществляется с территорий иностранных государств [2].

В докладе Президента Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства» на заседании Совета Безопасности Российской Федерации 20 мая 2022 г. отмечено, что с началом специальной военной операции вызовы в этой сфере стали ещё более острыми и серьёзными, более масштабными [3].

Указом Президента Российской Федерации от 22 декабря 2017 г. № 620 на Федеральную службу безопасности Российской Федерации (ФСБ России) возложены функции федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) [4, 5].

Рассматривается нормативно-правовое обеспечение создания, функционирования и современного этапа развития ГосСОПКА.

В начале 2000-х годов были созданы и отработаны технологии и механизмы информационного взаимодействия при реагировании на КА, компьютерные инциденты (КИ) и угрозы безопасности в отношении защищаемых ИР.

В 2011 году был создан Центр реагирования на КИ в органах государственной власти.

В январе 2013 года было принято решение о создании ГосСОПКА [6], а в Концепции ГосСОПКА [7] определены назначение, функции и принципы создания ГосСОПКА, а также виды обеспечения, необходимые для ее создания и функционирования.

Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [8] перед ФСБ России была поставлена задача совершенствования ГосСОПКА, в том числе — создание национального координационного центра по КИ (НКЦКИ). Требования федерального закона в рамках полномочий ФСБ России [5] реализованы соответствующими приказами [9 — 14].

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации в рамках своих полномочий [15] утвердило Порядок установки и эксплуатации средств, предназначенных для поиска признаков КА в сетях электросвязи, используемых для организации взаимодействия объектов КИИ, и Технические условия установки и эксплуатации средств, предназначенных для поиска признаков КА в сетях электросвязи, используемых для организации взаимодействия объектов КИИ [16].

Указом Президента Российской Федерации от 1 мая 2022 г. № 250 [17] определены дополнительные меры по обеспечению информационной безопасности Российской Федерации, направленные, в том числе, на развитие ГосСОПКА с учетом актуальных угроз безопасности в отношении ИР, которые в рамках полномочий ФСБ России [5] реализованы соответствующими приказами [18, 19], а также разрабатываются проекты: положения об аккредитации центров ГосСОПКА; требований к центрам ГосСОПКА и порядка контроля за деятельностью аккредитованных центров ГосСОПКА; порядка информирования ФСБ России о КИ и КА, связанных с функционированием ИР органов (организаций); порядка, технических условий установки и эксплуатации в ИР органов (организаций) средств, предназначенных для поиска признаков КА.

Федеральным законом от 14 июля 2022 г. № 266-ФЗ [20] статья 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» дополнена частью 12 [21], которая обязывает оператора персональных данных в порядке, определенном ФСБ России, обеспечивать взаимодействие с ГосСОПКА, включая информирование его о КИ, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных. Приказом ФСБ России от 13 февраля 2023 г. № 77 утвержден порядок взаимодействия операторов с ГосСОПКА, включая информирование ФСБ России о КИ, повлекших неправомерную передачу персональных данных [22].

Нормативно-правовое обеспечение современного этапа развития государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации характеризуется динамичным развитием с учетом меняющихся угроз в информационной сфере, что создает условия для обеспечение защищенности информационных ресурсов (ИС, ИТКС и АСУ) от компьютерных атак и обеспечения их штатного функционирования в условиях возникновения компьютерных инцидентов, вызванных целевыми компьютерными атаками.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).
2. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 2 июля 2021 г. № 400).
3. Доклад Президента Российской Федерации В. В. Путина 20 мая 2022 г. на заседании Совета Безопасности Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства».
4. «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» : Указ Президента Российской Федерации от 20 декабря 2017 г. № 620.
5. Положение о Федеральной службе безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 11 августа 2003 г. № 960 «Вопросы Федеральной службы безопасности Российской Федерации»).
6. «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» : Указ Президента Российской Федерации от 15 января 2013 г. № 31с (выписка).
7. Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274).
8. «О безопасности критической информационной инфраструктуры Российской Федерации» : Федеральный закон от 26 июля

2017 г. № 187-ФЗ.
9. «Об утверждении Положения о Национальном координационном центре по компьютерным инцидентам» : Приказ ФСБ России от 27 августа 2018 г. № 366.
10. «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» : Приказ ФСБ России от 24 июля 2018 г. № 367.
11. «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» : Приказ ФСБ России от 24 июля 2018 г. № 368.
12. «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» : Приказ ФСБ России от 6 мая 2019 г. № 196.
13. «Об утверждении Порядка, технических условий установки и эксплуатации средств предназначенных, для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» : Приказ ФСБ России от 19 июня 2019 г. № 281.
14. «Об утверждении порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятии мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» : Приказ ФСБ России от 19 июня 2019 г. № 282.
15. Положение о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации (утв. постановлением Правительства Российской Федерации от 2 июня 2008 г. № 418).
16. «Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» : Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 17 марта 2020 г. № 114.
17. «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» : Указ Президента Российской Федерации от 1 мая 2022 г. № 250.
18. «Об определении переходного периода, предусмотренного подпунктом «б» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 250» : Приказ ФСБ России от 1 ноября 2022 г. № 543.
19. «Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации» : Приказ ФСБ России от 11 мая 2023 г. № 213.
20. «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности» : Федеральный закон от 14 июля 2022 г. № 266-ФЗ.
21. «О персональных данных» : Федеральный закон от 27 июля 2006 г. № 152-ФЗ (с изменениями и дополнениями).
22. «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных» : Приказ ФСБ России от 13.02.2023 № 77.

УДК 656.61

РАЗВИТИЕ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ИНТЕРЕСАХ ПРОМЫШЛЕННОСТИ В РОССИЙСКОЙ АРКТИКЕ

Митько Арсений Валерьевич[1], Сидоров Владимир Константинович[2]
[1]Арктическая общественная академия наук
Искровский пр., 22, офис 175, Санкт-Петербург, Россия, 193168
[1]Всероссийский научно-исследовательской институт метрологии имени Д. И. Менделеева
Московский пр., 19, Санкт-Петербург, Россия, 190005
[1] Северо-Западный институт управления – филиал РАНХиГС
Средний проспект В. О., 57/43, Санкт-Петербург, Россия, 199178
[2]Санкт-Петербургский университет ГПС МЧС России
Московский пр, 149, Санкт-Петербург, Россия, 196105
e-mails: arseny73@yandex.ru, hamradio-spb@yandex.ru

Аннотация. Рассматриваются актуальные вопросы обеспечения бесперебойной, надежной связью добывающих предприятий, расположенных в малонаселенных и малоосвоенных районах Крайнего Севера.

Ключевые слова: Крайний Север; месторождения; добывающие предприятия; радиорелейная связь; волоконно-оптическая связь; спутниковая связь; преимущества и недостатки различных видов связи в условиях Крайнего Севера; информация, телекоммуникация, инфраструктура; удаленные; малонаселенные территории; коренные малочисленные народы Севера.

DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE INTERESTS OF INDUSTRY IN THE RUSSIAN ARCTIC

Mitko Arseny[1], Sidorov Vladimir[2]
[1]Arctic Public Academy of Sciences
Iskrovskij Av., 22, office 175, Saint-Petersburg, Russia, 193168
[1]D. I. Mendeleev All-Russian research institute of metrology
Moskovskij Av., 19, Saint-Petersburg, Russia, 190005
[1]Northwestern Institute of Management RANE and PA
Sredny prospect V. O., 57/43, St. Petersburg, Russia, 199178
[2]Saint-Petersburg university of State fire service of EMERCOM of Russia
Moskovskij Av., 149, Saint-Petersburg, Russia, 196105
e-mails: arseny73@yandex.ru, hamradio-spb@yandex.ru

Abstract. The current issues of ensuring uninterrupted, reliable communication of mining enterprises located in sparsely populated and underdeveloped areas of the Far North are considered.

Keywords: The Far North; deposits; mining enterprises; radio relay communication; fiber-optic communication; satellite communication; advantages and disadvantages of various types of communication in the conditions of the Far North; information, telecommunications, infrastructure; remote; sparsely populated territories; indigenous peoples of the North.

Крайний Север, где расположены крупнейшие месторождения, крупные нефтегазодобывающие комплексы и предприятия по добыче полезных ископаемых, магистральные трубопроводы, занимает 70 % территории России и является стратегическим районом, имеющим жизненно важное значение для экономики страны, поэтому и вопрос обеспечения этих объектов и населенных пунктов надежными средствами и качественными услугами связи также имеет стратегическое значение.

Основными видами связи, используемой на Крайнем Севере страны, являются: радиорелейная, волоконно-оптическая и спутниковая связь, которые являются резервными друг для друга.

Показаны преимущества и недостатки рассматриваемых видов связи в суровых условиях Крайнего Севера. Однако в настоящее время обеспечение связью и телекоммуникационными услугами в некоторых районах Крайнего Севера не соответствует уровню развития инфотелекоммуникационных технологий в масштабе страны.

Учитывая высокие темпы совершенствования и достаточно высокую сменяемость информационных технологий, наиболее экономически эффективным становится не просто оказывать услуги или предоставлять в аренду каналы связи, а предоставлять комплексные информационно-сервисные услуги. Сегодня реализация наиболее эффективной экономической модели лежит в развитии транспортной инфраструктуры связи, активном продвижении широкополосного доступа в Интернет и других новациях.

Связь и телекоммуникационные услуги наиболее востребованы персоналом добывающих предприятий, оленеводами, геологами, коренным населением и населением отдаленных населенных пунктов районов Крайнего Севера и являются эффективным.

Одной из важнейших задач освоения природных богатств, а также социально-экономического развития Сибири, Дальнего Востока и Арктической зоны России, входящих в территорию Крайнего Севера, является построение современной информационно-телекоммуникационной инфраструктуры этого Мегарегиона страны [1].

В Арктической зоне Крайнего Севера России сосредоточены наибольшие запасы нефти и газа, а происходящее в настоящее время таяние полярных паковых льдов вследствие глобального потепления делает более реальными планы по их освоению. Из 6,2 млн км2 российского шельфа, предположительно, запасами нефти и газа обладают 6 млн км2, т. е. почти вся его территория. По некоторым оценкам в Арктической зоне России сосредоточена подавляющая доля общероссийских запасов золота — 40 %, нефти — 40 %, газа — 80 %, хрома и марганца — 90 % и т.д. Общая стоимость минерального сырья арктических недр превышает 30 трлн долларов [2].

Добыча и рациональное использование ресурсов Крайнего Севера, а также обеспечение потребностей проживающего здесь населения неразрывно связаны с дальнейшим развитием телекоммуникационной инфраструктуры, заменой морально устаревших видов связи с целью их полного соответствия современным требованиям.

Выбор технологии построения транспортной инфраструктуры связи на Крайнем Севере во многом предопределяется его природными особенностями: суровыми климатическими условиями; нестабильной геомагнитной обстановкой в высоких широтах; расположением участков добычи в труднодоступных местах; значительной удаленностью месторождений друг от друга и от головных предприятий; технологиями разведочного бурения; наличием или отсутствием автомобильных и железных дорог, линий электропередач; качеством и стоимостью реализации инфраструктуры связи. Например, после разведочного бурения или окончания добычи на месторождении оборудование необходимо перемещать в другое место, поэтому прокладка кабелей в таких случаях нецелесообразна и беспроводные решения обеспечения связью являются более быстрыми, простыми и экономически оправданными вариантами [3].

С учетом многих производственных, климатических, экономических и других факторов развития конкретных территорий на Крайнем Севере наиболее широкое распространение получили три технологии построения транспортной инфраструктуры оператора связи:

– радиорелейная связь;
– волоконно-оптическая связь;
– космическая связь.

Радиорелейная связь (РРС) прямой видимости является одним из наиболее экономичных и быстрых способов организации информационных потоков на большие расстояния. Работают станции РРС, как правило, в диапазоне частот 3,4÷11,7 ГГц. Их пропускная способность составляет 155 Мбит/с и более, а передача сигналов ведется с использованием многопозиционных видов модуляции.

Для современных магистральных и внутризоновых линий РРС характерно наличие системы дистанционного обслуживания, которая программно поддерживает уровень управления сетевыми элементами и сетью в целом, а также обеспечивает контроль, управление и техническое обслуживание оборудования [4].

В настоящее время преобладание РРС над проводными и спутниковыми технологиями связи в труднодоступных районах Крайнего Севера и расположенных выше 75 градусов северной широты обусловлено следующими факторами:

– большая и малоосвоенная территория Крайнего Севера;
– особенности ландшафта северных территорий;
– большие расстояния между населенными пунктами, месторождениями,
– промыслами, компрессорными станциями и т. п.;
– малочисленность потребителей услуг связи;
– более низкая стоимость связи.

Линии РРС прямой видимости легко пересекают труднодоступную местность Крайнего Севера. Кроме того, линии РРС наиболее эффективны при создании разветвленных сетей. Для обеспечения РРС прямой видимости антенны устанавливаются на мачтах (или башнях) на определенной высоте. Высоты мачт зависят от длины и географического профиля каждого интервала между соседними станциями и могут достигать 120 м. Строительство более высоких антенных мачт экономически невыгодно.

Теоретически промежуточные станции РРС можно устанавливать на расстоянии друг от друга от 40 до 60 км и более. Однако на практике мачты с антеннами радиорелейной связи устанавливаются на расстояниях от 20 до 40 км друг от друга, например, из-за необходимости установки РРС в конкретном пункте или, когда на трассе РРС имеются существенные препятствия различной природы, а также с учетом затухания сигнала из-за климатических особенностей для данной местности, например, при высокой влажности (дождь, туман, снег).

Системы радиосвязи позволяют гибко и оперативно охватывать большие территории, но при этом имеют ограниченную пропускную способность, что во многом обусловлено количеством частотных назначений, выданных тому или иному оператору.

Перспективными направлениями развития РРС являются использование пакетной передачи в радиокадре, использование более сложных схем модуляции (QAM-256, QAM-512), а также использование более высоких несущих частот в диапазонах 70–80 ГГц.

Использование диапазона 70–80 ГГц позволяет оборудованию РРС использовать доступную для передачи полосу частот 100 МГц, что в свою очередь позволяет достичь пропускной способности 1 Гбит/с. Существенным недостатком использования данного диапазона являются сильные затухания сигнала при атмосферных осадках, ограничивающие дальность связи в зависимости от климатических факторов до 2,5÷5 км при коэффициенте неготовности 0,001 %. Немаловажна ещё одна проблема, которая присуща РРС: загрузка диапазона радиочастот до 11 ГГц в настоящее время такова, что средства самой радиосвязи вынуждены работать в совмещенных диапазонах частот, но в этом диапазоне работают еще и средства радиолокации, радионавигации, радиотелеметрии. Таким образом, возникает серьезная и сложная административная проблема электромагнитной совместимости различных радиосредств, требующая решения не только в национальном, но и в международном масштабе [5].

СПИСОК ЛИТЕРАТУРЫ

1. Жители Крайнего Севера // Портал «Present5». [Электронный ресурс]. URL: https://present5.com/zhiteli-krajnego-severa-zhiteli-krajnegosevera-eto/ (дата обращения: 19.08.2023).
2. Ларченко Л. В. Современная Арктика: проблемы освоения и социальноэкономического развития // Региональная экономика: теория и практика, № 11 (194), март 2011. С. 2–8.
3. Гурлев И. В., Бородин В. А., Цыганов В. В. Управление развитием информационно-телекоммуникационной инфраструктуры Сибири, Дальнего Востока и Арктики // ИТНОУ (Информационные технологии в науке, образовании и управлении), 2019. № 2. С. 15–19.
4. Основы проектирования цифровых радиорелейных линий связи // М. А. Быховский [и др.] М. : Горячая линия-Телеком, 2014. 332 с.
5. Голиков А. М. Сети и системы радиосвязи и средства их информационной защиты : учеб. пособие. Томск: Томский гос. университет систем управления и радиоэлектроники, 2007. 392 с.

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 004.056:51

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ. ИСТОЧНИКИ ВОЗНИКНОВЕНИЯ, СРЕДСТВА И СПОСОБЫ ЗАЩИТЫ

Васютина Татьяна Львовна, Файзулин Алмаз Ильдарович
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: mvdinf7444822@yandex.ru

Аннотация. В данной статье рассматриваются проблемы случайных угроз информационной безопасности, источники. А также средства и способы защиты от несанкционированного доступа к источникам информации.

Ключевые слова: несанкционированный доступ; защита информации; безопасность информации; источники угроз безопасности информации.

THREATS TO INFORMATION SECURITY IN COMPUTER SYSTEMS. SOURCES OF OCCURRENCE, MEANS AND METHODS OF PROTECTION

Vasyutina Tatiana, Fayzulin Almaz
St. Petersburg University of the Ministry of Internal Affairs of Russia,
1 Pilot Pilyutova str., St. Petersburg, 198206, Russia
e-mail: mvdinf7444822@yandex.ru

Abstract. This article discusses the problems of accidental threats to information security, sources. As well as means and methods of protection against unauthorized access to information sources.

Keywords: unauthorized access; information protection; information security; sources of information security threats.

Актуальность угроз целостности и конфиденциальности информации требует внимательного отношения к задаче ее защиты. Данная статья рассматривает как случайные угрозы, так и способы их предотвращения.

Случайная угроза безопасности информации — непреднамеренные изменения изменение информации во время работы с ней. Источниками данной угрозы могут быть: помехи в линиях связи; сбои в программном обеспечении.

Преднамеренная угроза безопасности информации — действия нарушителя выполнив, которые он получит доступ или изменит целостность охраняемой информации [1]. Источником угрозы будет выступать нарушитель безопасности информации.

Нарушитель безопасности информации — лицо, которое совершает действия с информацией, которые нарушают её безопасность при манипуляции с ней [2].

Есть следующие виды нарушителей:

– террористические, экстремистские организации;
– службы специального назначения иностранных государств;
– бывшие работники организаций.

Цели могут быть:

– организация террористических актов;
– нанесение ущерба общественному порядку;
– вмешательство в деятельность государства;
– месть бывшему работодателю.

Наиболее часто используемым видом нарушения безопасности информации, является несанкционированный доступ.

Несанкционированный доступ — действия с информации, которые нарушают правила обращения с информацией, например, нарушают конфиденциальность.

Наиболее распространённые способы несанкционированного доступа:

– перехват пароля;
– подбор пароля;
– применение вредоносных программ.

Перехват пароля осуществляется с помощью устройств ввода, то есть установки каких-либо программ, которые позволяют похитить пароль во время его ввода [3-4].

Подбор пароля может осуществлять путём перебирания всевозможных комбинаций или они могут выбираться из специальных словарей, в которых представлены самые распространённые комбинации.

Вредоносная программа — программа, которая предоставляет доступ к информации, без наличия на то права.

Для защиты компьютерной информации существует целый комплекс различных мер:

Организационные средства защиты, то есть затруднение или исключение утечки информации изнутри, например, ограничение доступа к информации не только посторонних лиц, но и персонала, или усиление защиты помещений, где хранятся носители информации.

Программные средства защиты, то есть использования различного рода программного обеспечения и программ для сохранности информации. Например, программы, которые при вводе пароля запрашивают «код подтверждения», который нужно ввести для продолжения работы с программой.

1. Технические средства, они связаны с помещением, где хранится информация и её обеспечение. Например, в данной комнате могут быть различного рода «глушилки» электромагнитных сигналов.

2. Правовые средства защиты — это регулирование при помощи нормативно правовых актов правил обращения с информацией. Например, в Уголовном Кодексе Российской Федерации появляются стать, которые предполагают ответственность за разглашение или незаконное получение информации.

Таким образом, в современном мире уже существует множество способов получения информации, и они постоянно развиваются, это означает, что для обеспечения безопасности нужно быть более аккуратным при посещении различных сайтов и подключения каких-нибудь внешних носителей к своему компьютеру. Также нужно постоянно совершенствовать средства защиты информации, что подразумевает, как техническое обеспечение, так и правовое регулирование.

СПИСОК ЛИТЕРАТУРЫ

1. Вострецова Е. В. Основы информационной безопасности : учеб. пособие для студентов вузов. Екатеринбург : Изд-во Урал. ун-та, 2019. 204 с.
2. Галатенко В. А. Основы информационной безопасности. М. : Интернет-Университет Информационных Технологий. ИНТУИТ. РУ, 2013.
3. Галатенко В. А. Стандарты информационной безопасности. М. : Интернет-Университет Информационных Технологий. ИНТУИТ. РУ, 2004.
4. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. М. : Издательство Молгачева С. В., 2001.

УДК 004.056:51

СИСТЕМА УПРАВЛЕНИЯ ЭЛЕКТРОННЫМИ КУРСАМИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Воронов Сергей Алексеевич, Примакин Алексей Иванович
Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: voronov-sci@mail.ru, aprimakin@mail.ru

Аннотация. Рассматривается вопрос о применении системы управления электронными курсами в образовательных организациях силовых структур, с учетом особенностей размещения ресурса и доступа к ним участникам образовательного процесса.

Ключевые слова: информационно-образовательная среда; электронный учебно-методический комплекс; дистанционное обучение; система контроля знаний; тестирующие программы; управление обучением.

ELECTRONIC COURSE MANAGEMENT SYSTEM IN THE CONTEXT OF DIGITALIZATION OF EDUCATIONAL ACTIVITIES

Voronov Sergey, Primakin Alexey
St. Petersburg Military Order of Zhukov Institute of National Guard Troops of the Russian Federation
1 Pilyutov's pilot St., St. Petersburg, 198206, Russia
e-mail: voronov-sci@mail.ru, aprimakin@mail.ru

Abstract. The issue of the application of the electronic course management system in educational organizations of law enforcement agencies is considered, taking into account the peculiarities of resource placement and access to them to participants of the educational process.

Keywords: educational environment of the university; electronic educational and methodological complex; distance learning; knowledge control system; learning management.

Процесс цифровизации образования в очередной раз подтолкнул образовательные организации к переводу большей части учебно-методического обеспечения в цифровую форму или пересмотру имеющихся механизмов хранения и обработки информации такого рода. Сейчас техническое оснащение и доступность сети Интернет (или внутренних сетей организации) перестали быть насущей проблемой. Современное образование сочетает в себе элементы очного и заочного обучения, оно становиться все более мобильным, динамичным и электронным. Значительно повышается роль электронной информационно-образовательной среды (ЭИОС) образовательной организации, которая в условиях электронного или дистанционного

обучения становится главным инструментом взаимодействия с обучающимися. Размещение организационной и планирующей документации на соответствующем информационном ресурсе организации является одной из составляющих ЭИОС, но далеко не самой значимой. Учитывая руководящие документы, определяющие состав и структуру ЭИОС, обязательными элементами среды являются учебно-методический комплекс и система контроля знаний [1].

Сложившиеся условия санкционного давления и ограничения по использованию программных продуктов не входящих в реестр российских программ для ЭВМ и баз данных еще раз подчеркнули потребность в гибком инструментарии, который позволял бы обеспечивать совместный доступ к учебно-методическому комплексу всех участников образовательной деятельности, осуществлять педагогическую диагностику успеваемости обучающихся.

Особый интерес вызывает поиск программного обеспечения, удовлетворяющего потребности образовательных организаций в диагностическом аппарате при выполнении ряда условий или учитывая их. Для образовательных организаций государственных силовых структур помимо функциональности инструментария имеют значение такие вопросы как, экономическая целесообразность внедрения и сопровождения, доступность, отсутствие ограничений на использование (свободно распространяемое ПО и открытый исходный код), совместимость с различными операционными системами [2]. Сегодня на рынке ИТ существует не так много отечественных программ, выполняющих диагностические функции.

Компьютерное тестирование существенно дополняет традиционные методы диагностики, позволяет серьезно сэкономить время обработки полученных результатов, а также дает преподавателю достаточно широкий функционал по настройке параметров тестирования, таких как коэффициент сложности тестов, ограничение времени тестирования. Некоторые программные продукты позволяют использовать многовариантные вопросы, вопросы на установление верной последовательности, вопросы содержащие открытый ответ. Проведен сравнительный анализ распространённых программ и тестирующих комплексов, удовлетворяющих условиям: MyTest, Indigo, LMS Moodle [3].

Проведенный анализ указывает, что представленные программные решения в целом удовлетворяют минимальные потребности большинства образовательных организаций. Но существенным преимуществом обладает LMS Moodle, который давно себя зарекомендовал с положительной стороны. Имеющийся функционал позволяет создавать от простейших тестов до сложных (требующих детальной подготовительной работы), получать отчеты результатов прохождения теста или их попыток, пользоваться аналитическим инструментарием. Также играет существенную роль тот факт, что данный продукт с открытым кодом и распространяется по лицензии GNU (свободное распространение). Несмотря на то, что это далеко не новое решение, его внедрение в образовательных организациях силовых структур крайне низкое.

Система оценки знаний входит в учебно-методический комплекс и при системном подходе должна работать в взаимоувязке с другими элементами среды. Если учитывать этот фактор, решение на базе LMS Moodle представляет удачный вариант для реализации ЭИОС, так как это не просто тестирующая программа, а механизм с широким функционалом. Система контроля знаний является неотъемлемым элементом образовательной среды и служит инструментом для индикации достижения тех или иных уровней сформированности компетенций, которые определены в соответствующих образовательных стандартах и обозначены в основных образовательных программах. Выбор соответствующей системы контроля знаний остается за образовательной организацией и исходит из различных условий и факторов. Для государственных образовательных организаций по подготовке специалистов для силовых структур одними из важных критериев при выборе таких систем являются экономическая целесообразность и совместимость с отечественным программным обеспечением.

Процесс цифровой трансформации вынуждает пересмотреть существующие подходы к устоявшимся процессам. Анализ применяемых технологий и их адаптация позволит существенно повысить уровень цифровизации образовательной деятельности. Опыт использования Moodle в Санкт-Петербургском военном ордена Жукова институте ВНГ РФ позволил подтвердить его эффективность в условиях использования внутри ведомственной сети [4].

СПИСОК ЛИТЕРАТУРЫ

1. Бережнова Л. Н., Воронов С. А. Сущность и содержание педагогической диагностики компетенций // Вестник Воронежского государственного университета. Серия: Проблемы высшего образования. 2018. № 1. С. 39–42.
2. Воронов С. А., Бородавко А. В. Условия реализации дополнительных образовательных программ для специалистов силовых структур при использовании электронного обучения и дистанционных образовательных технологий // Вестник ВГУ. Серия : Проблемы высшего образования. 2022. № 3. С. 31-34.
3. Воронов С. А., Ефимова А. Б., Ракитский А. В. Выбор системы контроля знаний как неотъемлемого элемента электронной образовательной среды // V международная научно-практическая конференция (17 мая 2022 г.) : сборник научных статей. Санкт-Петербург, Петергоф : Федеральное государственное казенное военное образовательное учреждение высшего образования Военная академия материально-технического обеспечения имени генерала армии А. В. Хрулева Министерства обороны Российской Федерации, 2022. С. 460-469.
4. Воронов С. А., Рязанов Г. В. Электронная информационно-образовательная среда: опыт применения системы управления обучением MOODLE в военной образовательной организации // Вестник Санкт-Петербургского военного института войск национальной гвардии. 2021, № 1(14). С. 11-15.

УДК 342.7

ГОСУДАРСТВЕННОЕ ГАРАНТИРОВАНИЕ ПРАВ И СВОБОД ЛИЧНОСТИ, ПРАВОВЫЕ АСПЕКТЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Громова Ольга Владимировна
Фонд поддержки героико-патриотического воспитания молодежи
Черкасова ул. 4, Санкт-Петербург, 198052, Россия
e-mail: fund_shpey@mail.ru

Аннотация. Отсутствие нормативного закрепления принципа «баланс интересов» в правовых актах, посвященных национальной безопасности, актуализирует тематику гарантирования прав и свобод личности.

Статья посвящена выявлению аспектов гарантирования государством безопасности личности и конституционных прав и свобод.

Ключевые слова: гарантии прав и свобод, ограничение прав и свобод, безопасность, национальная безопасность, национальные интересы, баланс интересов личности, общества, государства.

STATE GUARANTEE OF INDIVIDUAL RIGHTS AND FREEDOMS, LEGAL ASPECTS OF NATIONAL SECURITY

Gromova Olga
Foundation for the Support of Heroic and Patriotic Education of Youth
Cherkasova str. 4, St. Petersburg, 198052, Russia
e-mail: fund_shpey@mail.ru

Abstract. The lack of normative consolidation of the principle of «balance of interests» in legal acts devoted to national security actualizes the topic of guaranteeing individual rights and freedoms. The article is devoted to the identification of aspects of guaranteeing the security of the individual and constitutional rights and freedoms by the state.

Keywords: guarantees of rights and freedoms, restriction of rights and freedoms, security, national security, national interests, balance of interests of the individual, society, state.

Введение. Права и свободы человека и гражданина гарантированы государством и установлены в Конституции Российской Федерации. В эти гарантии входит и стабильность экономики, отношений собственности, эффективность налоговой системы; и развитость институтов гражданского общества, демократический характер власти, политическая стабильность; правовые способы реализации и защиты прав и свобод. То есть вся совокупность правовых и политических институтов, средств, способов, механизмов и процедур, обеспечивающих реализацию, охрану и защиту прав и свобод человека, и гражданина.

Исследуя правовые гарантии безопасности личности, можно сделать вывод, что к совокупности конституционных норм, гарантирующих таковую во всех ее проявлениях, следует относить положения, регулирующие право на жизнь (ст. 20), запрет пыток, насилия и т. п. (ст. 21), право на свободу и личную неприкосновенность (ст. 22), право на защиту чести и достоинства (ст. 23), информационную безопасность (ст. 24), неприкосновенность жилища (ст. 25), свободу выбора национальности (ст. 26) и т.д., т. е. нормы главы 2, гарантирующие права и свободы человека и гражданина, поскольку реализация таковых в полной мере возможна лишь в состоянии безопасности личности.

Не допускается произвольного ограничения прав и свобод человека и гражданина в Российской Федерации, однако статей 55, все же допускается ограничение прав и свобод в отдельных случаях, предусмотренных федеральными законами. В этой же статье перечислены и угрозы, при которых такое ограничение возможно.

Одной из таких угроз является угроза безопасности государства и защиты законных интересов других лиц.

Необходимо отметить, что ограничение прав и свобод личности может быть применено исключительно в период действия особых правовых режимов – режима чрезвычайной ситуации и военного положения, когда нарушается «нормальная» жизнь государства и общества в целом. В любых иных случаях недопустимо ограничение прав и свобод личности, что гарантируется государством через систему права, судебную систему, систему общественных организаций и пр.

При этом гарантией от неоправданных и чрезмерных ограничений прав и свобод человека и гражданина является позиция Конституционного суда Российской Федерации: «опасность произвольного вторжения законодателя в сферу конституционных прав человека резко возрастает в условиях усиления террористической активности, социально-экономических, экологических кризисов и пандемий». По мнению Зорькина В.Д., ст. 55 Конституции Российской Федерации содержит общую формулировку, которая «таит в себе опасность неоправданно широкого толкования и установления на практике чрезмерных ограничений прав и свобод человека для защиты ценностей общего блага. Особенно если учитывать специфику российского менталитета, связанную с длительными традициями преобладания государственных и общественных интересов над личными интересами».

В монографии «Теория современной конституции» Т.Я. Хабриева и В.Е. Чиркин пишут: «не существует абсолютных прав и свобод, все они могут быть ограничены, но только на основе закона, в пределах, допускаемых

конституцией, в соответствии с требованиями международного права и в строго определенных целях <…>, (обеспечение общественного порядка, публичной морали, здоровья населения и т.п.)

Правовая позиция Конституционного суда Российской Федерации сводится к необходимости соблюдения следующих принципов: 1) ограничительные меры не должны быть чрезмерными, а только необходимыми и строго обусловленными целями; 2) ограничение не должно посягать на само существо того или иного права и приводить к утрате его реального содержания; 3) ограничения должны отвечать требованиям справедливости, являться адекватными, пропорциональными, соразмерными и необходимыми для защиты конституционно значимых ценностей; 4) норма федерального закона об ограничении прав должна быть формально определенной, точной, четкой и ясной, не допускающей расширительного толкования установленных ограничений и, следовательно, произвольного их применения.

Учитывая это, понятия «безопасность личности» должно быть содержать и представления о пределах ограничения прав и свобод граждан и включать в себя понятные и критерии таких ограничений. На сегодняшний день такие критерии в законодательстве Российской Федерации не выработаны.

Безопасность личности - это стабильное состояние защищенности конституционных прав и свобод человека и гражданина от внутренних и внешних угроз, которое позволяет в полной мере реализовать во всех сферах жизни человека.

Законом, безопасность рассматривается комплексно, куда входят и безопасность личности, и безопасность общества, и безопасность государства, это единая система из нескольких видов безопасности: такие как личная, национальная, экономическая, социальная, политическая, экологическая, информационная, международная и т.п. Этот список остается открытым.

В широком смысле безопасность является сложной системой противодействия внешним и внутренним угрозам, направленным на ухудшение существующего положения или осложнение функционирования определенных структур. К таким угрозам относятся:

– разведывательная и иная деятельность специальных служб и организаций иностранных государств, а также отдельных лиц, направленная на нанесение ущерба безопасности Российской Федерации;

– деятельность террористических организаций, группировок и отдельных лиц, направленная на насильственное изменение основ конституционного строя Российской Федерации, дезорганизацию нормального функционирования органов государственной власти (включая насильственные действия в отношении государственных, политических и общественных деятелей), уничтожение военных и промышленных объектов, предприятий и учреждений, обеспечивающих жизнедеятельность общества, устрашение населения, в том числе путем применения ядерного и химического оружия либо опасных радиоактивных, химических и биологических веществ;

– экстремистская деятельность националистических, религиозных, этнических и иных организаций и структур, направленная на нарушение единства и территориальной целостности Российской Федерации, дестабилизацию внутриполитической и социальной ситуации в стране;

– деятельность транснациональных преступных организаций и группировок, связанная с незаконным оборотом наркотических средств и психотропных веществ, оружия, боеприпасов, взрывчатых веществ;

– сохраняющийся рост преступных посягательств, направленных против личности, собственности, государственной власти, общественной и экономической безопасности, а также связанных с коррупцией.

Исходя из противодействия этим угрозам и формируются цели и задачи соответствующих государственных служб, создаваемых для обеспечения режима законности в государстве, в том числе путем ограничений.

Одной из немногочисленных попыток законодателя урегулировать процедуру введения законных ограничений прав и свобод находится в рамках борьбы с терроризмом и устанавливается Федеральным законом от 06.03.2006 № 35-ФЗ «О противодействии терроризму».

Статья 11 Закона содержит перечень конкретных мер и временных ограничений, которые могут вводиться в условиях режима контртеррористической операции, т. е. режима, преследующего цели пресечения и раскрытия террористического акта, минимизации его последствий и защиты жизненно важных интересов личности, общества и государства, вводимого и отменяемого по решению уполномоченного должностного лица. К таким мерам и ограничениям относятся: проверка у физических лиц документов, удостоверяющих их личность, а в случае отсутствия таких документов — доставление указанных лиц в органы внутренних дел Российской Федерации.

Так же прямое ограничение устанавливается Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 31.07.2023) «Об информации, информационных технологиях и о защите информации», статья «Ограничение доступа к информации».

Статья 4. Закона РФ от 27.12.1991 N 2124-1 «О средствах массовой информации» содержит следующие положения: «Не допускается использование средств массовой информации в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, материалов, пропагандирующих порнографию, насилие и жестокость, <…>«

Нельзя сказать, что законодательство Российской Федерации изобилует запретами или сколь-нибудь серьезными ограничениями прав и свобод человека, однако при разработке действующего Федерального закона

«О безопасности» законодатель отказался от такого фундаментального принципа, как принцип достижения баланса жизненно важных интересов личности, общества, государства, на котором в идеале должен строиться механизм обеспечения национальной безопасности в правовом государстве. Можно было бы отнести это к возрастающим политическим угрозам, однако дисбаланс в вопросах справедливости в приоритетах, связанных с жизненно важными интересами, составляет не меньшую угрозу для государственности, угрозу раскола в обществе.

Однако необходимо отметить, что интересы граждан раскрываются и защищаются не только и не столько законами о безопасности, сколько самой развитостью правоустанавливающих документов, среди которых – доктрины, стратегии, законы федерального и регионального уровней, которые несомненно учитывают различные аспекты жизни общества и интересов жизненных интересов каждого.

В частности, в Основах государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей, утвержденных Указом Президента РФ от 09.11.2022 № 809, конкретизируются отдельные положения Стратегии национальной безопасности РФ [8], направленные на защиту прав в культурной сфере; так же и положениями Доктрины информационной безопасности РФ (Указ Президента РФ от 05.12.2016 N 646); Стратегией противодействия экстремизму в РФ до 2025 года, Стратегией государственной национальной политики РФ на период до 2025 года, Основами государственной культурной политики [15], Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы, принятой Указом Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», Указом Президента Российской Федерации от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года»; Стратегии экономической безопасности, принятой Указом Президента РФ от 13.05.2017 № 208.

Это лишь небольшой перечень правовых актов, направленных на защиту широкого круга интересов в том числе интересов личности. Понимая ценность развитости правоотношений, уделяя внимание продуктивности системы гражданского общества, государственная политика в области безопасности предоставляет возможности для поиска и нахождения консенсуса интересов личности, общества и государства, несмотря на вызовы и угрозы современного мира.

Заключение. Может быть, как раз совокупные интересы людей, образующих нацию (народ), и составляют национальные интересы нашей страны, потому что люди - это первооснова государства, существование которого без народа невозможно, а, следовательно, государство должно исходить из интересов народа и его безопасности:

– укрепление обороны страны, обеспечение незыблемости конституционного строя, суверенитета, независимости, государственной и территориальной целостности Российской Федерации;

– укрепление национального согласия, политической и социальной стабильности, развитие демократических институтов, совершенствование механизмов взаимодействия государства и гражданского общества;

– повышение качества жизни, укрепление здоровья населения, обеспечение стабильного демографического развития страны;

– сохранение и развитие культуры, традиционных российских духовно-нравственных ценностей;

– повышение конкурентоспособности национальной экономики;

– закрепление за Российской Федерацией статуса одной из лидирующих мировых держав, деятельность которой направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях полицентричного мира.

СПИСОК ЛИТЕРАТУРЫ

1. Конституция Российской Федерации
2. Указ Президента РФ от 17.12.1997 N 1300 (ред. от 10.01.2000) «Об утверждении Концепции национальной безопасности Российской Федерации»
3. Указ Президента РФ от 10.01.2000 N 24 «О Концепции национальной безопасности Российской Федерации»
4. Указ Президента РФ от 12.05.2009 N 537 (ред. от 01.07.2014) «О Стратегии национальной безопасности Российской Федерации до 2020 года»
5. Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации»
6. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»
7. Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030»
8. Указ Президента РФ от 02.07.2021 N 400 «О Стратегии национальной безопасности Российской Федерации»
9. Закон РФ от 05.03.1992 г № 2446-1 (ред. от 26.06.2008) «О безопасности»
10. Федеральный закон № 390-ФЗ от 28.12.2010 года «О безопасности»
11. Федеральный закон от 06.03.2006 N 35-ФЗ (ред. от 10.07.2023) «О противодействии терроризму»
12. Федеральный закон от 25.07.2002 N 114-ФЗ (ред. от 28.12.2022) «О противодействии экстремистской деятельности»
13. Федеральный закон от 25.12.2008 N 273-ФЗ (ред. от 10.07.2023) «О противодействии коррупции»
14. Указ Президента РФ от 09.11.2022 N 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей»
15. Указ Президента РФ от 24.12.2014 N 808 (ред. от 25.01.2023) «Об утверждении Основ государственной культурной политики».
16. Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года».
17. Указ Президента РФ от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года».
18. Указ Президента РФ от 13.05.2017 N 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года»
19. Федеральный закон от 04.04.2005 N 32-ФЗ (ред. от 13.06.2023) «Об Общественной палате Российской Федерации».

20. Туранин В.Ю. «Национальные интересы: подходы к определению понятия; «Российская юстиция», 2021, N 1; Источник: СПС «Консультант Плюс»;
21. Холодная Е.В. «О правовом принципе баланса интересов личности, общества и государства»; Вестник Саратовской государственной юридической академии № 3 (122) 2018; С. 116-121
22. Адзиев Х.Г., Гасанов Н.Н. «Что такое «национальное согласие», или об опасности омонимии в политологии»; 2009 г Дагестанский государственный педагогический университет (Работа выполнена в рамках гранта Российского гуманитарного научного фонда 09-03-00816а/Р. Статья поступила в редакцию 19.07.2009 г)
23. Куричев А.А. «Основные проблемы ограничения прав человека в современном государстве в целях противодействия экстремизму и терроризму» С. 17-22; Источник: https://elar.urfu.ru/bitstream/10995/60551/1/978-5-7996-2407-1_02_04.pdf
24. Маникин Д.Н. «Защита прав личности - приоритетная тактическая цель уголовного процесса Российской Федерации»; Пермский филиал Санкт-Петербургского ИВЭСЭП, г. Пермь, «Историческая и социально-образовательная мысль.» Том 8 №5/1, 2016 С. 109-116
25. Феоктистов А.В., Зернов И.В. «Эволюция развития законодательства о национальной безопасности в российской федерации», Электронный научный журнал «Наука. Общество. Государство». 2023. Т. 11, № 1. http://esj.pnzgu.ru
26. Бабаджанян К. А. «Взаимная ответственность личности и государства как основа гармонизации взаимоотношений между ними (теоретико-правовой аспект», диссертация к.ю.н., «Саратовская государственная юридическая академия», г. Саратов, 2013 год
27. Шахов В.В. и др. «Политология курс лекций», Московский Университет МВД РФ им. В.Я. Кикотя, Источник: https://studfile.net/preview/16409179/page:15/
28. Командирова Т.Г. «Правовые гарантии безопасности личности в России», Вестник Саратовской государственной юридической академии · № 3 (92) · 2013 С. 51-54
29. Грецова Е.Е. «Ограничения прав и свобод человека в интересах обеспечения общественной безопасности и противодействия терроризму» Источник: https://www.sovremennoepravo.ru/
30. Хабриева Т. Я., Чиркин В. Е. Теория современной конституции. - Москва: Норма, 2005. - 320 с.

УДК 004.056:51

ПРИМЕНЕНИЕ АЛГОРИТМОВ ФАКТОРНОГО И ДИСПЕРСИОННОГО АНАЛИЗОВ ДЛЯ ФОРМИРОВАНИЯ И ВЫЯВЛЕНИЯ ПРИОРИТЕТНЫХ ФАКТОРОВ, ОПРЕДЕЛЯЮЩИХ УРОВЕНЬ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ПОДРАЗДЕЛЕНИЯХ СИЛОВЫХ СТРУКТУР

Ефимова Анна Борисовна, Примакин Алексей Иванович
Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: abefimova020770@mail.ru, a.primakin@mail.ru

Аннотация. Рассматривается вопрос о возможности применения алгоритмов факторного и дисперсионного анализов для формирования и выявления приоритетных факторов, определяющих уровень обеспечения защиты информации в подразделениях силовых структур.

Ключевые слова: информационная безопасность, алгоритмы факторного и дисперсионного анализов, показатели уровня обеспечения защиты информации.

APPLICATION OF FACTOR AND VARIANCE ANALYSIS ALGORITHMS FOR FORMATION AND IDENTIFICATION OF PRIORITY FACTORS DETERMINING LEVEL OF INFORMATION PROTECTION IN POWER UNITS

Efimova Anna, Primakin Alexey
St. Petersburg Military Order of Zhukov Institute of National Guard Troops of the Russian Federation
1 Pilyutov's pilot St., St. Petersburg, 198206, Russia
e-mail: abefimova020770@mail.ru, a.primakin@mail.ru

Abstract. The issue of the possibility of using algorithms of factor and variance analyses to form and identify priority factors determining the level of information protection in power units is considered.

Keywords: information security, algorithms of factor and variance analyses, indicators of the level of information protection.

Задача оценки и обеспечения соответствующего уровня защиты информации в структурных подразделениях силовых структур в настоящее время чрезвычайно актуальна и со стороны Департамента цифрового развития и защиты информации Росгвардии этой проблеме уделяется особое внимание [1, 2].

Анализ обзора состояния применения информационных технологий и технической защиты информации в Росгвардии в 2022 году [3] позволяет сформировать основную систему показателей, определяющих уровень обеспечения защиты информации в подразделениях силовых структур [4].

Существенную помощь в формировании на базе соответствующих показателей факторов и выявлении из них наиболее приоритетных, в большей степени определяющих уровень защиты информации, могут оказать алгоритмы и методики факторного и дисперсионного анализов [5].

Исходным материалом для факторного анализа служат корреляционные связи между переменными, в данном случае показатели, характеризующие состояние системы обеспечения защиты информации в соответствующем структурном подразделении, т.е. факторному анализу подвергаются корреляционные матрицы. Как правило, данные показатели могут быть измерены, имеют количественные размерности. В результате факторизации из корреляционной матрицы посредством специальных алгоритмов может быть извлечено необходимое количество факторов, которые как-бы «объединяют-группируют» исходные показатели-

переменные с высокими коэффициентами корреляции и не поддаются в дальнейшем непосредственному измерению.

Для выявления ведущих факторов и исключения факторов, оказывающих не существенное влияние на показатель уровня защиты информации в подразделении, применяются алгоритмы дисперсионного анализа, посредством разложения совокупной изменчивости (дисперсии) на отдельные компоненты, вызванные влиянием различных источников изменчивости.

Проведение факторного и дисперсионного анализов целесообразно и удобно проводить в среде специализированного программного обеспечения SPSS или STATISTICA.

СПИСОК ЛИТЕРАТУРЫ

1. Директива Росгвардии от 28 октября 2021 г. № Д-2 «О приоритетных направлениях деятельности войск национальной гвардии Российской Федерации в 2022 году» // Сайт Росгвардии. [Электронный ресурс] URL: https://rosguard.gov.ru/ (дата обращения: 28.09.2023).
2. В Москве откроют центр кибербезопасности Росгвардии. [Электронный ресурс] URL: https://www.vedomosti.ru/society/news/2021/04/27/867838-moskve-otkroyut-tsentr-kiberbezopasnosti-rosgvardii (дата обращения: 28.09.2023).
3. Обзор состояния применения информационных технологий и технической защиты информации в ВНГ РФ в 2022 году и основных направлений деятельности в установленной сфере на 2023 год. // Сайт Росгвардии. [Электронный ресурс] URL: https://rosguard.gov.ru/ (дата обращения: 28.09.2023).
4. Воронов С. А., Потапова Л. С., Примакин А. И. Оценка уровня готовности структурных подразделений силовых структур в области решения задач по применению информационных технологий и технологической защиты информации. Материалы VI-й международной научно-практической конференции «Инновационная железная дорога. Новейшие и перспективные системы обеспечения движения поездов. Проблемы и решения» : сб. статей / под общей ред. М. Г. Яшина. СПб : Петергоф : ВИ (ЖДВ и ВОСО), 2023. С. 275-286.
5. Большакова Л. В., Примакин А. И., Яковлева Н. А. Математико-статистические методы обработки экспериментальных данных при проведении научных исследований методические рекомендации. СПб : Изд-во СПб ун-та МВД России, 2014. 92 с.

УДК 004.056:51

ПРИМЕНЕНИЕ ТЕОРИИ ИГР ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОДРАЗДЕЛЕНИЯХ РОСГВАРДИИ

Ефимова Анна Борисовна, Примакин Алексей Иванович
Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: abefimova020770@mail.ru, a.primakin@mail.ru

Аннотация. Рассматривается вопрос о применении теории игр для обеспечения информационной безопасности в структурных подразделениях Росгвардии, в частности, для выбора средства эффективной защиты информационных систем от различного рода кибератак.

Ключевые слова: информационная безопасность, математические методы, теория игр, критерии Вальда и Гурвица.

APPLICATION OF GAME THEORY TO ENSURE INFORMATION SECURITY IN ROSGVARDIA UNITS

Efimova Anna, Primakin Alexey
St. Petersburg Military Order of Zhukov Institute of National Guard Troops of the Russian Federation
1 Pilyutov's pilot St., St. Petersburg, 198206, Russia
e-mail: abefimova020770@mail.ru, a.primakin@mail.ru

Abstract. The issue of applying the theory of games to ensure information security in the structural units of the Russian Guard, in particular, to choose a means of effective protection of information systems from various kinds of cyber attacks, is being considered.

Keywords: information security, mathematical methods, game theory, Wald and Hurwitz criteria.

Актуальность темы связана с необходимостью решения задач по обеспечению информационной безопасности в структурных подразделениях Росгвардии. Данному вопросу со стороны Департамента цифрового развития и защиты информации Росгвардии уделяется большое внимание [1, 2].

Для выбора средств эффективной защиты информационных систем ведомства от различного рода кибератак, необходим соответствующий математический инструментарий. Предлагаемая для этих целей теория игр, хорошо зарекомендовала себя во многих областях, решив достаточное количество разнообразных задач, в том числе и по обеспечению защиты информации [3, 4].

Теория игр предполагает наличие продавца и покупателя, в нашем случае, используемые средства защиты информации («продавец») и типы атак на информационную систему («покупатель»). Взаимосвязь между ними определяется платежной матрицей. Для формирования этой матрицы рассмотрим угрозы, предложенные специалистами в области информационной безопасности, с указанием вероятностей их проявления: Smurf-ping (31%), ICMP flood (10%), UDP flood (14%), TCP flood (11%), TCP SYN flood (31%) и прочие (3%) [5].

Средства защиты объекта информатизации могут быть следующие: файрволл (со стандартными настройками), средства обнаружения вторжения, резервирование канала связи и другие [6].

После построения платежной матрицы применяем критерии (например, Вальда или Гурвица), позволяющие определить средства эффективной защиты объекта информатизации от упомянутых выше типов атак. Однако, каждый из критериев имеет свои особенности, которые необходимо учитывать [7].

Критерий Вальда обеспечивает выбор «осторожной» стратегии: для каждого решения выбирается самая худшая ситуация и отыскивается гарантированный максимальный эффект, где полностью исключают риск. Данным критерием руководствуются лица, принимающие решение не склонные к риску.

Критерий Гурвица позволяет руководствоваться некоторым средним результатом эффективности, находящимся в поле между значениями по критериям «минимакса» и «максимина». Этот критерий используют те субъекты, которые хотят максимально точно идентифицировать степень своих рисковых предпочтений.

Таким образом, применяя теорию матричных игр и руководствуясь критериями Вальда и Гурвица, можно обеспечить наиболее оптимальный выбор средств защиты объекта информатизации структурного подразделения Росгвардии от различного рода кибератак.

СПИСОК ЛИТЕРАТУРЫ

1. О приоритетных направлениях деятельности войск национальной гвардии Российской Федерации в 2022 году : директива Росгвардии от 28 октября 2021 г. № Д-2 / Росгвардия [Электронный ресурс]. URL: https://rosguard.gov.ru/ (дата обращения: 28.07.2023).
2. В Москве откроют центр кибербезопасности Росгвардии. [Электронный ресурс]. URL: https://www.vedomosti.ru/society/news/2021/04/27/867838-moskve-otkroyut-tsentr-kiberbezopasnosti-rosgvardii (дата обращения: 28.07.2023).
3. Басараб М. А., Коннова Н. С. Теория игр в информационной безопасности: учеб.-метод. пособие. М.: МГТУ им. Н. Э. Баумана, 2019. 80 с. [Электронный ресурс]. URL: https://ibooks.ru/bookshelf/374903/reading (дата обращения: 28.07.2023).
4. Викснин И. И., Мариненков Е. Д., Чупров С. С. Применение теории игр для обеспечения безопасности коммуникации киберфизической системы с использованием механизмов репутации и доверия // Научно-технический вестник информационных технологий, механики и оптики, 2022. Т. 22. № 1. С. 47-59.
5. Число кибератак на информационные системы России выросло на 65 %. [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak (дата обращения: 28.07.2023).
6. Основные методы и способы защиты информации. [Электронный ресурс]. URL: https://itsec2012.ru/osnovnye-metody-i-sposoby-zashchity-informacii (дата обращения: 28.07.2023).
7. Принятие решений в условиях неопределённости. [Электронный ресурс]. URL: https://www.matematicus.ru/teoriya-sistem/prinyatie-reshenij-v-usloviyah-neopredelyonnosti (дата обращения: 28.07.2023).

УДК 378.095

О НЕОБХОДИМОСТИ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ПОДГОТОВКИ БУДУЩИХ ОФИЦЕРОВ РОСГВАРДИИ ДЛЯ РЕШЕНИЯ ЗАДАЧ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ЗАЩИТЫ НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ РОССИИ

Зозулин Игорь Николаевич, Примакин Алексей Иванович
Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: zozulin@mail.ru, a.primakin@mail.ru

Аннотация. Рассматривается вопрос о необходимости инженерно-технической подготовки будущих офицеров Росгвардии для решения задач по обеспечению информационной безопасности в системе защиты национальных интересов России с учетом сложных военно-политических условий в стране и современном мире.

Ключевые слова: информационные технологии, информационная безопасность, офицерские кадры Росгвардии.

ON THE NEED FOR ENGINEERING AND TECHNICAL TRAINING OF FUTURE ROSGVARDIA OFFICERS TO SOLVE PROBLEMS OF ENSURING INFORMATION SECURITY IN THE SYSTEM OF PROTECTING NATIONAL INTERESTS OF RUSSIA

Zozulin Igor, Primakin Alexey
St. Petersburg Military Order of Zhukov Institute of National Guard Troops of the Russian Federation
1 Pilyutov's pilot St., St. Petersburg, 198206, Russia
e-mail: zozulin@mail.ru, a.primakin@mail.ru

Abstract. The issue of the need for engineering and technical training of future officers of the Russian Guard to solve problems of ensuring information security in the system of protecting the national interests of Russia, taking into account the difficult military-political conditions in the country and the modern world, is being considered.

Keywords: information technology, information security, officers of the Russian Guard.

Актуальность темы связана, прежде всего с тем, что в сложных военно-политических условиях армии все больше требуются офицеры, способные реализовать программы реформирования современных войск и их развития [1].

Повышение эффективности подготовки будущих офицеров Росгвардии в ведомственных вузах становится актуальным вопросом формирования военно-профессиональных и профессиональных компетенций будущих военных специалистов, определяющихся потребностями военной службы [2].

Проведя анализ современного состояния подготовки офицерских кадров Росгвардии [3-5], можно наблюдать то, что будущим офицерам необходимы инженерно-технические знания.

При организации ведомственного обучения по направлению информационной безопасности необходимо учитывать и военно-политические условия, складывающиеся в стране, например, открытие в Москве главного центра информационных технологий войск национальной гвардии РФ, который создает и развивает

информационные системы, ПО и информационно-коммуникационную инфраструктуру, обеспечивает информационную безопасность и техническую защиту информации в войсках национальной гвардии России [6].

Необходимо обратить внимание на заявление главы Росгвардии Виктора Золотова, что ведомство получит дальнобойную артиллерию и танки. Он уточнил, что этот вопрос, который в данный момент «стоит очень остро», уже обсуждался с В. В. Путиным. Тяжелая техника будет включать в себя все то, что стояло на вооружении внутренних войск, — речь идет о закупках танков, БМП, БТР с артиллерийским вооружением, передвижных артиллерийских систем и зенитно-ракетных комплексов [7].

Данное обстоятельство еще раз подчеркивает крайнюю необходимость в формировании у офицеров Росгвардии, военно-профессиональных и профессиональных компетенций инженерно-технического профиля.

СПИСОК ЛИТЕРАТУРЫ

1. Цеханович Д. Б., Панкратов В. Каким быть современному военному образованию / Армейский сборник. 2022. № 12. [Электронный ресурс]. URL: http://army.ric.mil.ru/Stati/item/456129/ (дата обращения: 19.07.2023).
2. Александрова Е. А., Козлов О. А. Разработка модели совершенствования профессиональной подготовки курсантов Росгвардии // Проблемы современного образования. 2018. № 5. С. 193-201.
3. Гнутов А. Д. Подготовка будущих офицеров войск национальной гвардии Российской Федерации в области информационно-технологической безопасности. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/podgotovka-buduschih-ofitserov-voysk-natsionalnoy-gvardii-rossiyskoy-federatsii-v-oblasti-informatsionno-tehnologicheskoy (дата обращения: 19.07.2023).
4. Стрельцов Р. В., Лавина Т. А., Щегольков А. В. Цели и направления непрерывной подготовки офицерского состава войск национальной гвардии Российской Федерации в области применения средств информационных и коммуникационных технологий в служебно-профессиональной деятельности // Вестник ЧГПУ им. И. Я. Яковлева. 2017. № 3-1 (95). С. 173-179.
5. Усанин С. С., Усанин С. Н., Рузаев Н. В. Актуальные проблемы в подготовке специалистов в области технической защиты информации // Современные тенденции развития гуманитарных и социальных наук : сб. тр. Междунар. научно-практ. конф. с очным участием: в 2 ч. 2019. С. 275-283.
6. В Москве откроют центр кибербезопасности Росгвардии. [Электронный ресурс]. URL: https://www.vedomosti.ru/society/news/2021/04/27/867838-moskve-otkroyut-tsentr-kiberbezopasnosti-rosgvardii (дата обращения: 19.07.2023).
7. Танки для Росгвардии: законопроект о передаче ведомству военной техники внесен в Госдуму. [Электронный ресурс]. URL: https://bloknot.ru/politika/tanki-dlya-rosgvardii-zakonoproekt-o-peredache-vedomstvu-voennoj-tehniki-vnesen-v-gosdumu-1136459.html (дата обращения: 19.07.2023).

УДК 004.056

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОБЪЕКТЕ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Локнов Алексей Игоревич, Симакова Екатерина Андреевна
Санкт-Петербургский университет МВД России
Лётчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: info_for_aleksey@mail.ru, ekaterina.simakova.2001@yandex.ru

Аннотация. Рассматривается важность обеспечения информационной безопасности объекта критической информационной инфраструктуры (КИИ). В статье предлагаются меры для обеспечения безопасности значимых объектов. Критическая информационная инфраструктура играет важную роль в современном обществе, поскольку обеспечивают работоспособность критических систем и услуг, таких как энергетика, транспорт, телекоммуникации и финансы.

Ключевые слова: информационная безопасность, объект критической информационной инфраструктуры, меры обеспечения безопасности информации, уязвимость, угроза.

ENSURING INFORMATION SECURITY AT THE OBJECT OF CRITICAL INFORMATION INFRASTRUCTURE

Loknov Alexey, Simakova Ekaterina
Saint Petersburg University of the Ministry of internal Affairs of the Russian Federation
1 Pilyutov'spilot St., St. Petersburg, 198206, Russia
e-mails: info_for_aleksey@mail.ru, ekaterina.simakova2018@mail.ru

Abstract. The importance of ensuring the information security of a critical information infrastructure object is considered. The article proposes measures to ensure the safety of significant objects. Critical information infrastructure plays an important role in today's society as it keeps critical systems and services running, such as energy, transportation, telecommunications, and finance.

Keywords: information security, critical information infrastructure object, information security measures, vulnerability, threat.

В современном информационном обществе критическая информационная инфраструктура (КИИ) играет важную роль в обеспечении функционирования различных секторов экономики. Вмешательство в работу КИИ может привести к серьезным последствиям, таким как: нарушение работы крупных предприятий, утечка конфиденциальной информации или крупный материальный ущерб. Поэтому обеспечение информационной безопасности объектов КИИ становится приоритетной задачей государства.

Объекты критической информационной инфраструктуры (КИИ) — это информационные системы, сети и ресурсы, которые обеспечивают работу критически важных секторов экономики. Эти объекты могут включать системы управления энергетическими сетями, транспортные системы, финансовые платформы, системы связи и государственные информационные системы.

Уязвимости объектов КИИ могут возникать из-за недостатков в проектировании, реализации и эксплуатации информационных систем. Основные уязвимости включают отсутствие достаточного контроля доступа к системам, неэффективное управление учетными записями, недостаточную защиту сетевых связей, отсутствие мониторинга и обнаружения вторжений [1], а также отсутствие регулярного обновления программного обеспечения.

Меры по обеспечению информационной безопасности объектов КИИ включают:

– Определение классификации критической информации: Первым шагом в обеспечении безопасности объектов КИИ является анализ критической информации и её классификация по степени конфиденциальности и важности [2]. Это позволит определить, какие данные требуют наибольшей защиты. Важным шагом в обеспечении безопасности объектов КИИ является проведение комплексной оценки рисков и угроз. Это включает идентификацию потенциальных уязвимостей и угроз, анализ возможных последствий инцидентов безопасности, а также определение вероятности их возникновения. Результаты оценки рисков помогут разработать эффективные стратегии и меры по обеспечению безопасности.

– Разработку политик и процедур безопасности. Необходимо разработать и внедрить политики и процедуры безопасности, которые устанавливают требования к защите информации. Политики безопасности должны определяться с учетом специфических потребностей и угроз каждого объекта КИИ. Они должны охватывать такие аспекты, как управление доступом, управление учетными записями, шифрование данных, мониторинг и аудит безопасности.

– Физическую безопасность. Обеспечение физической безопасности объектов КИИ играет важную роль в предотвращении несанкционированного доступа к критическим системам и ресурсам. Это включает установку систем видеонаблюдения, контроля доступа, защиты помещений с серверами и сетевым оборудованием, а также обучение персонала вопросам физической безопасности.

– Защиту сетевой инфраструктуры. Сетевая инфраструктура объектов КИИ является ключевым элементом, требующим надежной защиты. Важно реализовать меры по обеспечению безопасности сети, такие как использование межсетевых экранов (firewalls), систем обнаружения вторжений (intrusion detection systems), систем предотвращения вторжений (intrusion prevention systems) и виртуальных частных сетей (Virtual Private Networks, VPN). Также необходимо регулярно обновлять и проверять сетевое оборудование и программное обеспечение, чтобы устранить известные уязвимости.

– Управление уязвимостями. Эффективное управление уязвимостями является неотъемлемой частью обеспечения информационной безопасности объектов КИИ. Это включает регулярное сканирование и анализ уязвимостей, а также исправление выявленных проблем [3]. Рекомендуется использовать автоматизированные инструменты для обнаружения и управления уязвимостями, а также следить за обновлениями.

Обучение и повышение осведомленности персонала являются важными аспектами обеспечения информационной безопасности. Персонал должен быть обучен базовым принципам безопасности информации, распознаванию фишинговых атак, использованию безопасных паролей и защите конфиденциальных данных [4]. Регулярные тренинги и осведомленность персонала помогут снизить риск внутренних угроз и ошибок.

Также регулярный аудит и мониторинг системы безопасности объектов КИИ необходимы для обнаружения и реагирования на потенциальные инциденты безопасности. Это включает мониторинг сетевого трафика, журналов событий и системных ресурсов [5]. Результаты мониторинга должны быть анализированы и своевременно реагировать на любые аномальные или подозрительные активности.

Эффективное обеспечение информационной безопасности объектов КИИ требует постоянного внимания и обновления. Организации, ответственные за КИИ, должны постоянно анализировать новые угрозы, применять передовые технологии и стандарты безопасности, а также обучать персонал. Только таким образом можно обеспечить надежную защиту объектов КИИ и предотвратить возможные угрозы и инциденты, которые могут иметь серьезные последствия для экономики и общества в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Вавичкин А. Н. К вопросу категорирования объектов критической информационной инфраструктуры // Безопасность информационных технологий, [S.l.]. Т. 26. № 2. 2019. С. 44–57. [Электронный ресурс] URL: https://www.elibrary.ru/item.asp?id=38568103 (дата обращения: 07.06.2023).
2. Гатчин Ю. А., Сухостат В. В. Информационная безопасность критической информационной инфраструктуры: теоретико-методологические аспекты // Инновационные, информационные и коммуникационные технологии : сборник трудов XVII Международной научно-практической конференции. Сочи, 01–10 октября 2020 года / под. ред. С. У. Увайсов. М. : Ассоциация выпускников и сотрудников ВВИА им. проф. Н. Е. Жуковского содействия сохранению исторического и научного наследия ВВИА им. проф. Н. Е. Жуковского, 2020. С. 213-217.
3. Сиротский А. А., Резниченко С. А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов // Безопасность информационных технологий. [S.l.]. Т. 28. № 3. С. 103–117, 2021. [Электронный ресурс] URL: https://www.elibrary.ru/item.asp?id=46709372 (дата обращения: 13.06.2023).
4. Чернова Е. В. Информационная безопасность человека : учеб. пособие для вузов. 2-е изд., испр. и доп. М. : Издательство Юрайт, 2023. 243 с. // Образовательная платформа Юрайт [сайт]. URL: https://urait.ru/bcode/518441 (дата обращения: 18.06.2023).
5. Бегишев И. Р. Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. 2019. № 1. С. 27–32.

УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВЕДОМСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Лопатин Богдан Владиславович, Якушев Денис Игоревич
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: bogdamilian@gmail.com, d.i.ya@yandex.ru

Аннотация. Рассматриваются меры и средства защиты ведомственных информационных систем на объекте информатизации ОВД, информационная безопасность и факторы, способствующие ее повышению в органах внутренних дел Российской Федерации.

Ключевые слова: информационная безопасность, информационная система, органы внутренних дел, защита информации, средства защиты информации.

INFORMATION SECURITY AUDIT AS A MEASURE OF INFORMATION PROTECTION AT THE ATS INFORMATIZATION FACILITY

Lopatin Bogdan, Yakushev Denis
St. Petersburg University of the Ministry of Internal Affairs of Russia
1 Letchik Pilyutov St, St. Petersburg, 198206, Russia
e-mails: bogdamilian@gmail.com, d.i.ya@yandex.ru

Abstract. Measures and means of protecting departmental information systems at the object of informatization of internal affairs bodies, information security and factors contributing to its improvement in the internal affairs bodies of the Russian Federation are considered.

Keywords: information security, information system, internal affairs bodies, information protection, information security means.

На сегодняшний день информационное обеспечение органов внутренних дел Российской Федерации является одним из основополагающих направлений. Постоянно продолжается оснащение техническими современными комплексами и системами с последующим вовлечением их в повседневную практическую деятельность.

Несмотря на то, что к настоящему времени был проведен большой объем работ по информационному обеспечению органов внутренних дел, обеспечение требуемого уровня информационной безопасности пока еще не соответствует требованиям времени.

Информационная безопасность ведомственных информационных систем

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [2].

Информационная безопасность систем органов внутренних дел — это защищенность всех информационных ресурсов в информационных системах МВД России, которые защищают интересы страны.

Одна из главных задач — исключить внешнее программное воздействие на систему. Программное воздействие — несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ [1].

Первое и основное, на что необходимо обратить внимание при обеспечении информационной безопасности любой сферы, связанной с информацией, это то, что необходимо достичь трех главных задач безопасности, которые применяются ко всем видам информации:

– конфиденциальность;
– целостность;
– доступность.

Угрозы информационной безопасности для ведомственных информационных систем можно классифицировать на внутренние и внешние. Говоря о внутренних угрозах необходимо отметить то, что человеческий фактор являлся, является и будет являться одной из главных угроз любых информационных систем, не только ведомственных. Так будет до тех пор, пока все системы не придут к полной автоматизации работы. Внешними угрозами, в свою очередь, чаще всего, являются современные кибератаки хакеров.

Зачастую в России происходят масштабные сбои федеральных или ведомственных информационных систем, например, сбой информационной системы Госавтоинспекции. По этой причине возникли проблемы с регистрацией автомобилей и выдачей водительских удостоверений.

В прошлом году в работе федеральных информационных систем ГИБДД также произошли несколько сбоев. Технические проблемы возникали по линии предоставления государственных услуг по регистрации транспорта и выдаче водительских удостоверений. Для противодействия таким сбоям необходим активный союз с институтами гражданского общества, государственными учреждениями, бизнесом, интернет-сообществом.

Также, необходимы высококвалифицированные кадры в МВД России. Нехватка хорошего уровня специалистов в данной сфере создает проблему, которая, в свою очередь, плавно переходит в угрозу информационной безопасности Российской Федерации.

Для каждой ведомственной информационной системы следует подготовить нормативно-правовую документацию. Необходимо создать план, который будет учитывать:

– количество работающих компьютеров в подразделении, включая сломанные устройства, которые в ремонте;
– как проходит ремонт сломанных компьютеров, кто принимает участие в данной работе;
– как проходит процесс списания и утилизации устройств, а также процесс введения в эксплуатацию новых устройств.

Технология блокчейн — это усовершенствованный механизм базы данных, который позволяет организовать открытый обмен информацией в рамках бизнес-сети [3]. В 2023 году глава Росфинмониторинга доложил Путину о запуске «прозрачного блокчейна» в правоохранительных органах. Эта новость, безусловно, положительный момент для органов внутренних дел Российской Федерации. Но необходимо и учитывать недостатки данной технологии:

– масштабируемость;
– блокчейн может потреблять большое количество энергии;
– возможность осуществления атаки 51%;
– цепочка блоков не имеет возможности изменения данных в уже добавленных блоках, что может быть недостатком, если произошли какие-то ошибки или были внесены ошибочные данные;
– блокчейн, являющийся открытым и прозрачным реестром, также может вызывать некоторые вопросы, которые касаются приватности пользователей;
– многие сотрудники ОВД пока не готовы к децентрализованным технологиям или пока не понимают концепцию блокчейна, что создает преграды для массового принятия разработки и ее использования.

Именно после того, когда каждый сотрудник, который будет работать с данными технологиями, разберется в полной мере с недостатками, тогда можно будет сделать вывод о том, что первый шаг к повышению уровня информационной безопасности данной ведомственной системы сделан.

Таким образом, можно сделать вывод, что обеспечение информационной безопасности ведомственных информационных систем — это то, на что сегодня необходимо обратить внимание, в первую очередь для того, чтобы обеспечить информационную безопасность государства и успешную работу правоохранительных органов. Каждый сотрудник, который имеет отношение к работе с ведомственными информационными системами, должен четко понимать все риски такой работы и в полной мере разбираться с ее функционалом.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200057516 (дата обращения: 05.10.2023).
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Доступ из справочно-правовой системы «Консультант-плюс».
3. Шурыгин В. А., Ядыкин И. М. Принципы и методы технологии блокчейн в приложении к криптовалютаму : учеб. пособие. Национальный исследовательский ядерный университет «Московский инженерно-физический институт», 2020. 116 с.

УДК 004.056:51

ЗАЩИТА ДАННЫХ В ЦИФРОВОЙ ЭПОХЕ

Милованов Андрей Сергеевич, Шалагинова Ольга Борисовна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: flowwei6@gmail.com shalaginova1337@yandex.ru

Аннотация. В эпоху цифровой трансформации информационная безопасность стала одним из наиболее актуальных и стратегически важных вопросов, стоящих перед государствами, компаниями и каждым отдельным гражданином. Вместе с неоспоримыми преимуществами, которые приносит с собой цифровая революция, появились и новые угрозы, связанные с хищением данных, кибератаками и нарушением частной жизни. В таком контексте не только важно разработать соответствующие меры по защите информации, но и строгое законодательство, регулирующее эти меры. С ростом числа киберугроз и нарушений конфиденциальности данных становится ясным, что необходимо обеспечить эффективную правовую защиту как для индивидуальных прав и свобод, так и для бизнес-процессов и функционирования государства в целом. В данной статье мы подробно рассмотрим ключевые аспекты, связанные с правовыми мерами в области информационной безопасности и их влияние на общество.

Ключевые слова: информационная безопасность; законы о защите данных; международное сотрудничество; контроль и надзор; цифровая эпоха.

DATA PROTECTION IN THE DIGITAL AGE

Milovanov Andrew, Shalaginova Olga
St. Petersburg University of the Ministry of Internal Affairs of Russia
1 Pilot Pilyutova St, St. Petersburg, 198206, Russia
e-mail: flowwei6@gmail.com shalaginova1337@yandex.ru

Abstract. In the era of digital transformation, information security has become one of the most pressing and strategically important issues facing nations, companies and every individual citizen. Along with the undeniable benefits that the digital revolution brings with it, new threats of data theft, cyberattacks and privacy violations have also emerged.

In such a context, it is not only important to develop appropriate measures to protect information, but also strict legislation governing these measures. With the increasing number of cyber threats and data privacy breaches, it is clear that there is a need to provide effective legal protection for both individual rights and freedoms, as well as for business processes and the functioning of the state as a whole. In this article, we take a closer look at key aspects related to legal measures in the field of information security and their impact on society.

Keywords: Information security; data protection laws; international cooperation; control and supervision; the digital age.

В цифровую эпоху защита данных становится одной из ключевых задач обеспечения информационной безопасности в Российской федерации. Данные представляют собой ценный ресурс, который может быть использован как для достижения социальных, экономических и культурных целей, так и для нанесения ущерба интересам государства, организаций и граждан. Правовые аспекты защиты данных включают в себя как международные, так и национальные нормы, и стандарты, регулирующие сбор, обработку, хранение, распространение и уничтожение данных, а также права и обязанности субъектов данных, операторов данных и поставщиков услуг. Основными проблемами в этой области являются баланс между правом на частную жизнь и правом на информацию, защита персональных данных в сети Интернет, ответственность за нарушение защиты данных и сотрудничество между государствами и организациями в борьбе с киберпреступностью. Для решения этих проблем необходимо разработать и применять эффективные правовые механизмы, основанные на уважении прав человека, принципах демократии и верховенства закона.

В Российской Федерации информационная безопасность выступает в качестве приоритетного направления государственной политики. В этой связи очень важна разработка эффективной концепции Стратегии кибербезопасности Российской Федерации. В настоящее время Стратегия развития информационного общества В РФ рассчитана до 2030 г [1]. В информационной безопасности нуждаются все отрасли экономики, сферы государственного управления, органы обороны и охраны правопорядка. Данная ситуация связана, в том числе, с цифровизацией их деятельности, созданием единой системы госуслуг.

Необходимость особого подхода к информационной безопасности связана с развитием информационно телекоммуникационных технологий, потребностью в обеспечении защиты информации, в том числе персональной информации, информации, составляющей какой-либо вид тайны. Важный вопрос на сегодняшний день — регулирование деятельности электронных средств массовой информации, обеспечение свободного доступа к некоторым видам информации и т.д. Важна также защита коммерческой и информации, которая используется бизнесом. Одним словом, если не будет обеспечен надлежащий уровень информационной безопасности, функционирование многих систем будет попросту невозможным.

Доктрина информационной безопасности представляет собой совокупность официальных взглядов на цели, задачи, направления развития политики в сфере информационной безопасности РФ. Она служит основанием не только для формирования политики в данной сфере, но также и для разработки предложений по совершенствованию правового, методического, научно-технического и иного обеспечения информационной безопасности.

Доктрина закрепляет четыре основных национальных интереса России в области информационной среды:

– Соблюдение прав и свобод человека и гражданина, закрепленных в Конституции РФ, касательно Получения информации, а также ее использования.

– Информационное обеспечение политики страны, как внутренней, так и внешней.

– Развитие современных информационных технологий, в том числе отечественного производства, направленных на информатизацию, развитие телекоммуникаций и связи, обеспечение потребности внутреннего рынка, выход отечественной информационной продукции на мировой рынок.

– Защита имеющихся информационных ресурсов от несанкционированного доступа.

В доктрине упоминаются правовые, экономические и организационно технические методы, которыми обеспечивается информационная безопасность страны [2]. Так. к правовым методам относится нормативно-правовая база РФ, которая регламентирует отношения в информационной сфере, и, в том числе, устанавливает уголовную и административную ответственность за совершение информационных правонарушений. Организационно-технические методы направлены на создание системы информационной безопасности, разработку новых технических продуктов, предупреждение несанкционированного доступа к информации и т.д. Экономические методы направлены на определение порядка финансирования вопросов обеспечения информационной безопасности, создание системы страхования информационных рисков юридических и физических лиц.

Правовые аспекты информационной безопасности играют важную роль в защите данных и обеспечении безопасности в цифровой эпохе. Законы о защите данных, киберзаконодательство, контроль и надзор, международное сотрудничество и образование — все эти элементы совместно способствуют созданию надежного и устойчивого киберпространства [3]. Важно соблюдать эти правовые нормы и продолжать развивать меры по обеспечению информационной безопасности, чтобы защитить наши данные и обеспечить безопасность в цифровом мире.

СПИСОК ЛИТЕРАУРЫ

1. Правовые аспекты информационной безопасности / под ред. А. В. Мальцева. М.: Юристъ, 2019.
2. Правовые основы обеспечения информационной безопасности Российской Федерации : учеб. пособие / под ред. А. В. Мальцева, А. А. Степанова, В. И. Королева ; Российский университет дружбы народов (РУДН). М. : РУДН, 2021. 240 с.
3. Правовое обеспечение информационной безопасности РФ / под ред. В. И. Королева, А. В. Мальцева, А. А. Степанова. М. : Юристъ, 2020. 432 с.

УДК 378.147

ПУТИ ЗАЩИТЫ И МЕРЫ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЕ ЗАКОНА О ПЕРСОНАЛЬНЫХ ДАННЫХ

Парфенов Николай Петрович, Шалагинова Ольга Борисовна, Карпов Павел Евгеньевич
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: parfenov-nikolai@mail.ru, shalaginova1337@yandex.ru, best-man82@mail.ru

Аннотация. Приведены пути защиты персональных данных и меры ответственности за нарушение закона о персональных данных в современных условиях. Раскрыты основные положения доктрины информационной безопасности. Приведены виды ответственности за нарушение закона о персональных данных.

Ключевые слова: персональные данные, информационная безопасность, доктрина информационной безопасности, меры ответственности.

WAYS OF PROTECTION AND MEASURES OF RESPONSIBILITY FOR VIOLATION OF THE LAW ON PERSONAL DATA

Parfenov Nikolai, Shalaginova Olga, Karpov Pavel
St. Petersburg University of the Ministry of Internal Affairs of Russia
1 Pilyutov's pilot St., St. Petersburg, 198206, Russia
e-mail: parfenov-nikolai@mail.ru, shalaginova1337@yandex.ru, best-man82@mail.ru

Abstract. Ways to protect personal data and penalties for violating the law on personal data in modern conditions are given. The main provisions of the information security doctrine are revealed. The types of liability for violation of the law on personal data are given.

Keywords: personal data, information security, information security doctrine, liability measures.

В 2016 г. президент Российской Федерации В. В. Путин подписал указ № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [1]. В Доктрине перечислены основные пути достижения информационной безопасности нашей страны. Одной из мер обеспечения информационной безопасности является защита персональных данных, далее (ПДн), которая включает различные методы и способы.

В настоящее время социальные сети широко привлекаются не только для личного общения, но и для решения производственных задач. Чаще всего, социальные сети применяются для поиска кандидатов на работу. Кандидат на работу (далее пользователь) обязан предоставлять свои персональные данные. Каким же образом кандидат на работу сможет обеспечить свою безопасность от мошенников и преступников в социальных сетях?

На данный момент применяются следующие меры защиты — применение механизмов безопасности социальных сетей и эксплуатация общих механизмов защиты компьютера.

Применение механизмов безопасности социальных сетей означает, например, дать доступ к одному из своих альбомов всем пользователям, а к другому — только друзьям.

Эксплуатация общих механизмов защиты компьютера подразумевает использование защищенного протокола взаимодействия с Web-серверами.

Например, при входе и пребывании в социальной сети необходимо использовать протокол https. Данная операция обеспечивает безопасную передачу информации по сети. Кроме этих операций необходимо установить на компьютер и на мобильные устройстваантивирусные программы и некоторые средства защиты.

Кроме всего прочего, при общении в сети необходимо соблюдать элементарные меры безопасности, например, не добавлять малознакомых людей в друзья.

Отдельно необходимо отметить социальную инженерию, которая применяется для получения информации. На практике, создается определенная ситуация, в которой пользователи сами выкладывают злоумышленникам сведения.

На данный момент, защита персональных данных — вопрос далеко не новый, но в тоже время еще нерешенный в нашей стране. На всех уровнях можно встретить беспечное отношение к персональным данным, как у пользователей, так и у учреждений, работающих с конфиденциальной информацией пользователей.

В современных условиях действующий Федеральный закон «О персональных данных» не очень эффективно используется на практике. На данный момент нет ни одного резонансного уголовного дела, связанного с нарушением требований настоящего ФЗ-152.

К справедливости необходимо отметить, что угрозы нарушения конфиденциальности, целостности и доступности наших персональных данных существовали и до принятия ФЗ-152 от 27.07.2006 г. «О персональных данных» [2].

После утверждения и принятия этого закона все равно оставалось и остается множество незакрытых «дыр» в области защиты ПДн. Поэтому, на сегодняшний день ФСТЭК, ФСБ и Роскомнадзор (регуляторы по безопасности ПДн) утвердили документы по обеспечению защиты наших с вами ПДн.

В соответствии со статьей 23 ФЗ-152 «О персональных данных», уполномоченным органом по защите прав субъектов персональных данных является Роскомнадзор. На сегодняшний день, Роскомнадзор осуществляет проверку организационно-распорядительных документов организации на соответствии выполнения требований по защите ПДн.

Как мы видим по сообщениям из открытых источников, что утечки ПДн носят весьма объемный характер и нанесение ущерба субъекту персональных данных (определение места жительства, раскрытие его доходов и т.д.) может нанести непоправимый ущерб и не только материальный (экономический), но и репутационный. В связи с этим проблема защиты стала не только личного характера, но и огромной проблемой государства, как ущерб национальным интересам.

Многие организации в РФ стараются обеспечивать, если уже не обеспечили защиту ПДн не только своих клиентов, но и своих работников. Но многим предстоит пройти эту процедуру.

Какие же меры ответственности предусмотрены на данный момент за нарушение закона о персональных данных? Перечислим лишь основные виды:

- Административная (ст. 5.39, 13.11, 13.14, 19.5 и 19.7 КоАП РФ);
- Уголовная (ст. 137, 140 и 272 УК РФ);
- Дисциплинарная (пп. «в» п. 6 ст. 81 ТК РФ);
- Материальная (ст. 238 ТК РФ);
- Гражданско-правовая.

Таким образом, в современных условиях для защиты персональных данных используются различные методы и способы: технические, правовые, организационные, социальные. Кроме этого, существуют и применяются меры ответственности за нарушение закона о персональных данных.

СПИСОК ЛИТЕРАТУРЫ

1. Указ № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
2. ФЗ-152 от 27.07.2006 г. «О персональных данных».

УДК 004.056

ФОРМИРОВАНИЕ СИСТЕМЫ ПОКАЗАТЕЛЕЙ, ОПРЕДЕЛЯЮЩИХ СТЕПЕНЬ ЗАЩИТЫ ИНФОРМАЦИИ СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ РОСГВАРДИИ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Потапова Людмила Сергеевна, Примакин Алексей Иванович
Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: Ly-da.83@mail.ru, a.primakin@mail.ru

Аннотация. Рассматривается система показателей, характеризующих уровень готовности структурных подразделений Росгвардии для решения задач цифровой трансформации и по обеспечению защиты информации в современных условиях информационного противоборства.

Ключевые слова: защита информации в подразделении Росгвардии; цифровая трансформация; система показателей, характеризующих уровень защиты информации.

FORMATION OF A SYSTEM OF INDICATORS DETERMINING THE DEGREE OF INFORMATION PROTECTION OF ROSGVARDIA STRUCTURAL UNITS IN CONDITIONS OF INFORMATION CONFRONTATION

Potapova Ludmila, Primakin Alexey
St. Petersburg Military Order of Zhukov Institute of National Guard Troops of the Russian Federation
1 Pilyutov's pilot St., St. Petersburg, 198206, Russia
e-mail: Ly-da.83@mail.ru, a.primakin@mail.ru

Abstract. A system of indicators is being considered that characterize the level of readiness of the structural units of the Russian Guard to solve the problems of digital transformation and to ensure the protection of information in modern conditions of information confrontation.

Keywords: information protection in the Rosgvardia division; digital transformation; a system of indicators characterizing the level of information protection.

Основные усилия Департамента цифрового развития и защиты информации Росгвардии с учетом приоритетных задач, определенных директивой Росгвардии от 28 октября 2021 г. № Д-2 «О приоритетных направлениях деятельности войск национальной гвардии Российской Федерации в 2022 году» были направлены на обеспечение информационной безопасности и технической защиты информации в ВНГ РФ [1].

Проведя анализ обзора состояния применения информационных технологий и технической защиты информации в Росгвардии в 2022 году и основных направлений деятельности в установленной сфере на 2023 год [2], были определены основные показатели.

Первый показатель связан с количеством личного состава соответствующего подразделения, прошедшего обучение по профильным программам повышения квалификации [3].

Следующие два показателя отражают степень реализации лимитов бюджетных обязательств и технического обеспечения структурных подразделений Росгвардии в соответствии с табелем положенности необходимым оборудованием, средствами автоматизации и защиты информации.

Следующий, четвертый показатель связываем с проведением мероприятий по аттестации единого информационного пространства войск для обработки информации ограниченного распространения.

Пятый показатель — доля АРМ, переведенных на использование отечественной операционной системы [4].

Шестой — совершенствования механизма межведомственного электронного взаимодействия с органами государственной власти соответствующего структурного подразделения Росгвардии [5].

Эти показатели имеют отношение, в первую очередь, к правовым и организационно-техническим методам обеспечения защиты информации.

Следующая группа показателей напрямую характеризует состояние информационной безопасности. Это наличие: антивирусной защиты; системы обнаружения вторжений; программно-аппаратного комплекса межсетевого экранирования; подсистемы поиска уязвимостей [6].

Полнота предложенных показателей, оценки обеспечения информационной безопасности с точки зрения отражения всех возможных вариантов не является исчерпывающей.

СПИСОК ЛИТЕРАТУРЫ

1. О приоритетных направлениях деятельности войск национальной гвардии Российской Федерации в 2022 году : директива Росгвардии от 28 октября 2021 г. № Д-2 // Росгвардия. [Электронный ресурс]. URL: https://rosguard.gov.ru/ (дата обращения: 20.07.2023).
2. Обзор состояния применения информационных технологий и технической защиты информации в ВНГ РФ в 2022 году и основных направлений деятельности в установленной сфере на 2023 год // Росгвардия. [Электронный ресурс]. URL: https://rosguard.gov.ru/. (дата обращения: 20.07.2023).
3. Федеральный проект «Кадры для цифровой экономики» национальной программы «Цифровая Экономика Российской Федерации» // Росгвардия. [Электронный ресурс]. URL: https://rosguard.gov.ru/ (дата обращения: 20.07.2023).
4. Распоряжение Росгвардии от 10 авг. 2022 г. № 1/1284-р. // Росгвардия. [Электронный ресурс]. URL: https://rosguard.gov.ru/ (дата обращения: 20.07.2023).
5. Об оружии : Федер. закон от 13 дек. 1996 г. № 150-ФЗ // Росгвардия. [Электронный ресурс]. URL: https://rosguard.gov.ru/ (дата обращения: 20.07.2023).
6. План проведения анализа защищенности информационных ресурсов ЕИП Росгвардии // Росгвардия. [Электронный ресурс]. URL: https://rosguard.gov.ru/ (дата обращения: 20.07.2023).

УДК 004.415.25

АНАЛИЗ УГРОЗ КИБЕРБЕЗОПАСНОСТИ В ОБЛАСТИ ЗДРАВООХРАНЕНИЯ

Пронский Александр Юрьевич, Шалагинова Ольга Борисовна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: pronskiy04@gmail.com, shalaginova1337@yandex.ru

Аннотация. В данной статье рассмотрена одна из наиболее актуальных проблем в настоящее время — это кибербезопасность в области здравоохранения. Приведён список последствий, к которым могут привести угрозы кибербезопасности медицинских учреждений. Разработаны дальнейшие направления исследований в области кибербезопасности в здравоохранении. Для защиты рекомендуется использовать сильные пароли, двухфакторную аутентификацию, регулярно обновлять программное обеспечение.

Ключевые слова: кибербезопасность; здравоохранение; социальная инженерия; конфиденциальная информация; финансовая информация.

ANALYSIS OF CYBERSECURITY THREATS IN THE FIELD OF HEALTHCARE

Pronsky Alexander Yurievich, Shalaginova Olga Borisovna
St. Petersburg University of the Ministry of Internal Affairs of Russia,
1 Pilot Pilyutova str., St. Petersburg, 198206, Russia
e-mail: pronskiy04@gmail.com, shalaginova1337@yandex.ru

Abstract. This article discusses one of the most pressing problems at the present time — this is cybersecurity in the field of healthcare. The list of consequences to which threats to the cybersecurity of medical institutions can lead is given. Further directions of research in the field of cybersecurity in healthcare have been developed. For protection, it is recommended to use strong passwords, two-factor authentication, and regularly update the software.

Keywords: cybersecurity; healthcare; social engineering; confidential information; financial information.

Кибербезопасность в области здравоохранения является одной из наиболее актуальных проблем в настоящее время [1]. С каждым годом количество кибератак на медицинские учреждения растет, что может привести к серьезным последствиям для пациентов и медицинских работников.

В этой статье мы рассмотрим различные виды угроз, с которыми сталкиваются медицинские учреждения, а также методы защиты от этих угроз. Мы также обсудим последствия кибератак на медицинские учреждения и пациентов, а также рассмотрим дальнейшие направления исследований в области кибербезопасности в здравоохранении.

В области здравоохранения существует множество угроз кибербезопасности [2], которые могут привести к серьезным последствиям для пациентов и медицинских учреждений. Некоторые из наиболее распространенных угроз включают в себя:

– Фишинг и социальная инженерия. Эти атаки направлены на обман пользователей, чтобы они раскрыли конфиденциальную информацию или установили вредоносное ПО.

– Уязвимости медицинского оборудования. Медицинское оборудование, такое как мониторы жизненно важных функций и насосы для инфузий, может быть подвержено кибератакам, что может привести к серьезным последствиям для пациентов.

– Угрозы со стороны внутренних пользователей. Внутренние пользователи, такие как медицинский персонал и административный персонал, могут представлять угрозу безопасности, если они не следуют правилам безопасности или если их учетные данные были скомпрометированы.

– Риски, связанные с использованием сторонних поставщиков услуг. Медицинские учреждения могут использовать сторонних поставщиков услуг для хранения и обработки конфиденциальной информации, что может привести к риску ее утечки.

– Проблемы с безопасностью мобильных устройств. Мобильные устройства, такие как смартфоны и планшеты, могут быть подвержены кибератакам, что может привести к утечке конфиденциальной информации.

Вот частичный список тех последствий, к которым могу привести угрозы кибербезопасности учреждений здравоохранения:

– Утечка конфиденциальной информации. Кибератаки могут привести к утечке конфиденциальной информации, такой как медицинские записи, личные данные пациентов и финансовая информация.

– Нарушение работы медицинского оборудования. Кибератаки могут привести к нарушению работы медицинского оборудования, такого как мониторы жизненно важных функций и насосы для инфузий, что может привести к серьезным последствиям для пациентов.

– Риск для жизни пациентов. Кибератаки могут представлять риск для жизни пациентов, если они приводят к нарушению работы медицинского оборудования или утечке конфиденциальной информации.

– Негативное влияние на репутацию. Кибератаки могут негативно сказаться на репутации медицинских учреждений и привести к потере доверия со стороны пациентов и общественности.

Некоторые известные атаки на учреждения здравоохранения по всему миру включают в себя:

– WannaCry: В 2017 году WannaCry стал одной из самых широко распространенных кибератак на мировые системы здравоохранения. Атака зашифровала данные больниц и требовала выкуп за их восстановление.

– NotPetya: В 2017 году NotPetya атаковал многие учреждения здравоохранения, включая больницы в США и Великобритании. Атака привела к тому, что многие больницы были вынуждены отменить операции и прием пациентов.

– Ryuk: В 2019 году Ryuk был использован для атак на несколько больниц в США. Атака привела к тому, что больницы были вынуждены перейти на ручное управление.

Существует множество других атак на учреждения здравоохранения, которые не были упомянуты здесь. Чтобы защититься от таких атак, рекомендуется использовать сильные пароли, двухфакторную аутентификацию, регулярно обновлять программное обеспечение и обучать персонал основам кибербезопасности.

В заключение можно подвести итоги и описать дальнейшие направления исследований. Необходимо разрабатывать новые методы защиты, которые могут эффективно защитить медицинские учреждения от кибератак. Медицинские учреждения должны обучать своих пользователей правилам безопасности и методам защиты от кибератак. Новые технологии, такие как искусственный интеллект [3], могут быть использованы для обеспечения безопасности данных в медицинских учреждениях. Для более глубокого понимания проблем кибербезопасности в области здравоохранения необходимо проводить дополнительные исследования.

СПИСОК ЛИТЕРАТУРЫ

1. Всемирная организация здравоохранения. Проект глобальной стратегии в области цифрового здравоохранения на 2020-2025 гг. ВОЗ. Женева. 2020. 39 с. [Электронный ресурс]. URL: https://www.who.int/docs/default-source/documents/200067-draft-global-strategy-on-digital-health-2020-2024-ru.pdf (дата обращения: 04.10.2023).
2. Клебанов Л. Р., Полубинская С. В. Цифровое здравоохранение, пандемия covid-19 и проблемы кибербезопасности // Вестн. Том. гос. ун-та. 2021. № 468. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/tsifrovoe-zdravoohranenie-pandemiya-covid-19-i-problemy-kiberbezopasnosti (дата обращения: 04.10.2023).
3. Всемирная организация здравоохранения. Этика и управление искусственным интеллектом в интересах здоровья. ВОЗ. Женева. 2021 г. [Электронный ресурс]. URL: https://www.who.int/ru/news/item/28-06-2021-who-issues-first-global-report-on-ai-in-health-and-six-guiding-principles-for-its-design-and-use (дата обращения: 04.10.2023).

УДК 343.98

ОБ АСПЕКТАХ ПРИМЕНЕНИЯ НЕКРИМИНАЛИСТИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Проурзина Ольга Юрьевна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: cemiramida@mail.ru

Аннотация. Рассматриваются аспекты раскрытия и расследования преступлений с применением некриминалистических информационных систем. Социальные сети, открытые данные, базы данных финансово-кредитных организаций позволяют получить доказательства совершения правонарушения.

Ключевые слова: цифровая трансформация; закон и порядок; открытые данные.

ASPECTS OF THE USE OF NON-CRIMINALISTIC INFORMATION SYSTEMS

Prourzina Olga
St. Petersburg University of the Ministry of Internal Affairs of Russia
Pilyutov's pilot St., 1, St. Petersburg, 198206, Russia
e-mail: cemiramida@mail.ru

Abstract. Aspects of the disclosure and investigation of crimes using non-criminalistic information systems are considered. Social networks, open data, databases of financial and credit organizations allow you to obtain evidence of an offense.

Keywords: digital transformation; law and order, open data.

Цифровизация современного мира, развитие всемирной информационно-телекоммуникационной компьютерной сети «Интернет», локальных информационных сетей и специализированных информационных систем представляет большие ресурсы для развития человечества. Рациональное использование данных из открытых источников, а также информационных систем, эксплуатируемых вне ведения Министерства внутренних дел Российской Федерации может успешно применяться для борьбы с преступностью.

Период конца XX — начала XXI вв. в мировой истории, а также в истории Российской Федерации характеризуется стремительным развитием информационных технологий, выраженным в появлении платформ передачи информации с возможностью обмена не только текстовыми сообщениями, но и фото-, видеоматериалами, а также записи речевых, вербальных звуковых сигналов. Цифровая информация, хранящаяся вне служебных информационных систем может представлять интерес при раскрытии и расследовании преступлений и сборе доказательств.

Немаловажное значение при раскрытии и расследовании преступлений имеет любая информация, которая может предоставить сведения о событии преступления или стать доказательством по делу. В условиях ограниченного времени для раскрытия и расследования преступления сотрудники органов внутренних дел задействуют все доступные ресурсы для получения сведений и сбора доказательств. В этих целях направляются запросы в действующие и архивные некриминалистические информационные системы, т.е. базы данных и информационные массивы неслужебного назначения.

На сегодняшний день каждый человек может себе позволить оставаться онлайн или же иметь периодический доступ к выходу в информационно-коммуникационную сеть «Интернет» (далее — сеть «Интернет»). Также, возросла скорость передачи данных, что, до недавнего времени, оставалось невозможным. Однако, наряду с повышением уровня жизни населения, как следствие развития телекоммуникационных технологий, возрастает и уровень преступности. Такого рода преступления совершаются на почве информационных взаимоотношений, складывающихся в сети «Интернет» [5]. Злоумышленники активно используют возможности технологического прогресса в своих преступных целях, раскидывая свои электронные сети и вовлекая в них лиц, которые подвергаются данному воздействию, не имея со своей стороны какого-либо умысла на совершение преступлений.

Всемирная информационно-телекоммуникационная сеть «Интернет» представляет особый интерес для граждан, осуществляющих противоправную деятельность. Оставаясь незамеченными, они долгое время могут совершать преступные деяния, в надежде избежать наказания. Одним из самых распространенных видов незаконной деятельности, осуществляемой через сеть «Интернет», является незаконный оборот наркотических средств, психотропных веществ, аналогов, прекурсоров, психоактивных и запрещенных веществ. В настоящее время данный вопрос стоит как никогда остро именно с развитием информационных технологий и трансформированием классических форм и методов совершения данных преступлений посредством перехода в удаленную онлайн среду мессенджеров и вебсайтов. Причина, по которой данные составы преступлений наделены повышенным вниманием и контролем со стороны государства и государственных органов всех уровней, а также общественности, кроется не только в сущности этих преступлений, которая заключается в подрыве здоровья и генофонда населения, но и в общественной опасности данного деяния [5].

Правоохранительными органами ежегодно выявляется около 200 тыс. преступлений данной категории, их удельный вес в общем количестве зарегистрированных преступлений составляет порядка 10%, из незаконного оборота изымается более 20 тонн наркотиков [2]. В процессе анализа судебной практики, а также практики,

сложившейся в результате производства предварительного расследования, мы пришли к выводу о том, что злоумышленники совершают преступления рассматриваемой категории, выполняя действия объективной стороны, по большей части, с наркотическими средствами и психотропными веществами. Таким образом, при рассмотрении указанного вида преступлений, преимущественно, речь будет идти именно о незаконном обороте наркотических средств и психотропных веществ, как о наиболее распространенных предметах преступных посягательств, совершаемых с использованием сети «Интернет» и электронных средств оплаты.

Способы и методы совершения преступлений в сфере незаконного оборота наркотиков с использованием сети «Интернет» и электронных средств оплаты постепенно усложняются, этому способствуют трансграничные способы передачи информации, анонимные платежные системы, а также способы передачи информации через различные каналы связи. Это происходит из-за технологического прогресса, который позволяет злоумышленникам, используя научные достижения, создавать и применять новые схемы распространения наркотиков. Сотрудники правоохранительных органов не всегда владеют профессиональными знаниями в области информационно-коммуникационных технологий и эксплуатации средств связи для раскрытия правонарушений в кратчайшие сроки. Разнообразный спектр оконечных устройств связи пользователей, различные программные решения для передачи коротких текстовых сообщений (мессенджеров) позволяет правонарушителям скрывать свои криминальные деяния.

При раскрытии и расследовании преступлений сотрудниками органов внутренних дел именно абонентские устройства и метаданные, содержащиеся в их файловой структуре, а также цифровые «следы» пользователей в сети «Интернет» будут иметь важное значение при установлении лица подозреваемого в совершения преступления и сборе доказательств преступления. Криминалистически значимая информация может содержаться в информационных системах юридических и частных лиц, которая в дальнейшем будет собрана и проанализирована на этапе сбора доказательств. Ведомственные информационные системы органов внутренних дел представляют собой упорядоченные массивы данных, которые подразделяются на криминалистические учеты, оперативно-розыскные учеты, информационно-справочные учеты и иные служебные информационные системы. Получение сведений из служебных информационных систем является строго регламентированной процедурой и проводится на всех этапах раскрытия и расследования преступлений. Применение сторонних информационных систем, имеющих значимую для раскрытия и расследования информацию, но функционирующих вне ведения правоохранительных органов, сопряжено с расходованием ресурсов и не всегда может быть реализовано в дистанционном формате.

На этапе доследственной проверки и предварительного расследования обязательно собираются достаточные сведения, необходимые для доказывания признаков преступного деяния, а также дающие право говорить об устойчивости и сплоченности, выразившимися в общности криминальных интересов и целей групп лиц, заключавшихся в извлечении материальной прибыли в результате совершения незаконного сбыта наркотических средств, наличии общих денежных средств, полученных в результате преступной деятельности, которые аккумулировались на счетах «QIWI-кошельков», наличии системы конспирации и защиты от правоохранительных органов, которая выражалась в том, что незаконный сбыт наркотических средств осуществлялся бесконтактным способом под вымышленными именами с использованием обозначений вместо фактических названий сбываемого товара [7]. Также, при расследовании преступлений рассматриваемой категории распространёнными случаями являются совершение действий, содержащих в себе признаки состава преступления, предусмотренного ст. 174.1 УК РФ — легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления. Ошибочным решением должностного лица является оставить данные действия без соответствующей квалификации.

Так, действия по переводу полученных в результате купли-продажи наркотиков электронных денежных средств или криптовалюты, поступивших на электронный кошелек посредством их перевода напрямую или через «Dark net», на банковскую карту или другой электронный кошелек лично продавцом или при помощи программного софта с целью дальнейшего обналичивания, следует квалифицировать по вышеуказанной статье, как легализация денежных средств, приобретенных лицом в результате незаконного сбыта наркотиков [6].

Таким образом, при расследовании уголовных дел в сфере незаконного оборота наркотиков, совершенных с использованием сети «Интернет» и электронных средств оплаты, требуется обращать внимание на фактические обстоятельства дел с целью установления сведений, которые являются обязательными в доказывании по данным делам. Это обеспечит полноту и всесторонность рассмотрения уголовных дел, как следствие, соблюдение и обеспечение защиты конституционных прав и свобод человека и гражданина.

Актуальность данной темы исследования обусловлена развитием информационных технологий, что приводит к росту числа преступлений, в том числе, связанных с незаконным оборотом наркотиков, посредством создания новых способов и методов их совершения. Данный рост приводит к повышению наркотизации подрастающего поколения, то есть тех слоев населения, здоровье и развитие которых представляют повышенный интерес государства [4]. Повышение употребления наркотиков ведет к снижению интеллектуальных способностей населения, что в долгосрочной перспективе может сказаться на национальной безопасности Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. «О наркотических средствах и психотропных веществах» : Федеральный закон от 08.01.1998 № 3-ФЗ (ред. от 08.12.2020) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система [офиц. сайт]. URL: http://www.consultant.ru/ (дата обращения: 22.01.2021).
2. «Об оперативно-розыскной деятельности» : Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 30.12.2020) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система [Офиц. сайт]. URL: http://www.consultant.ru/ (дата обращения: 05.01.2021).

3. «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации до 2030 года» : Указ Президента РФ от 23.11.2020 № 733 // Собрание законодательства РФ. 30.11.2020. № 48. Ст. 7710.
4. «О Стратегии национальной безопасности Российской Федерации» : Указ Президента РФ от 31.12.2015 № 683 // Собрание законодательства РФ, 04.01.2016. № 1. Ст. 212.
5. Тертычная И. В., Бадзгарадзе Т. А., Проурзина О. Ю. Особенности выявления, раскрытия и расследования преступлений в сфере незаконного оборота наркотических веществ, совершенных с использованием информационно-коммуникационной сети «Интернет» // Аграрное и земельное право. 2022. № 9 (213). С. 113-117.
6. Щурова А. С. Незаконный оборот наркотических средств и их аналогов с исрользованием компьютерных технологий (сети Интернет) : уголовно-правовое и криминологическое исследование. СПб, 2017. 256 с.
7. Яшин А. В., Шикшеев В. Р. Проблемы противодействия преступлениям в сфере незаконного оборота наркотиков, совершаемым посредством сети Интернет // Вестник Пензенского государственного университета. П., 2020. № 3 (31). С. 107-112.
8. Приговор Абаканского городского суда Республики Хакасия от 27.07.2020 по уголовному делу № 1-647/2020, в отношении гражданина М., осужденного в совершении преступления, предусмотренного ч. 2 ст. 210, ч. 3 ст. 30 п. п. «а, г» ч.4 ст.228.1 УК РФ // [Электронный ресурс]. URL: https://sudact.ru/regular/doc/M9CqqOBPiP5m/ (дата обращения 20.12.2020).

УДК 004.056

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК МЕРА ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ ОВД

Рогова Юлия Николаевна, Якушев Денис Игоревич
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: yulyasha1603@mail.ru, d.i.ya@yandex.ru

Аннотация. Рассматриваются меры и средства защиты информации на объекте информатизации ОВД, аудит информационной безопасности, как одна из эффективных мер защиты информации и проблемы осуществления аудита.

Ключевые слова: аудит информационной безопасности, объект информатизации, органы внутренних дел, защита информации, меры защиты информации.

INFORMATION SECURITY AUDIT AS A MEASURE OF INFORMATION PROTECTION AT THE ATS INFORMATIZATION FACILITY

Rogova Yuliya, Yakushev Denis
St. Petersburg University of the Ministry of Internal Affairs of Russia
1 Letchik Pilyutov St, St. Petersburg, 198206, Russia
e-mails: yulyasha1603@mail.ru, d.i.ya@yandex.ru

Abstract. The measures and means of information protection at the ATS informatization facility, information security audit, as one of the effective measures of information protection and the problems of audit implementation are considered.

Keywords: information security audit, informatization object, internal affairs bodies, information protection, information protection measures.

Век информационных технологий создал самостоятельный тип актива — информацию. Как любая ценность, информация подвергается посягательствам со стороны различных мошенников. Существенные риски возникают и в области обеспечения государственной безопасности в сфере информации. Органы внутренних дел владеют очень большим объемом информации, которая не должна становиться доступной неопределенному кругу лиц и уж тем более попадать в руки к злоумышленникам, поэтому объекты информатизации ОВД требуют осуществления мер по обеспечению информационной безопасности и наличия функционирующих средств защиты информации.

Аудит информационной безопасности

Под объектом информатизации следует понимать совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [1].

В Министерстве внутренних дел Российской Федерации и других организациях, занимающихся правопорядком и безопасностью, обеспечение информационной безопасности играет критическую роль. К основным средствам и мерам защиты информации, которые могут использоваться в МВД, стоит отнести: сетевую защиту (например, фильтрация сетевого трафика и мониторинг сетевых активностей, фаерволы и интранет-системы для ограничения доступа к сети, виртуальные частные сети (VPN) для безопасного удаленного доступа); антивирусное и антималварное программное обеспечение (установка и обновление антивирусных программ на всех компьютерах и серверах, регулярное сканирование и удаление вредоносных программ); обеспечение физической безопасности информационных ресурсов (ограничение доступа к серверным и коммуникационным комнатам, использование систем контроля доступа и видеонаблюдения); шифрование данных; идентификация и аутентификация; регулярное обновление и обучение (регулярное обновление операционных систем и

прикладного программного обеспечения, обучение сотрудников правилам безопасности); инцидентное реагирование и многое другое.

Как известно из федерального закона «Об информации, информационных технологиях и о защите информации», защита информации представляет собой принятие правовых, организационных и технических мер [2]. Одной из задач организационного обеспечения защиты информации является выработка критериев и определение порядка проведения оценочных мероприятий по установлению степени эффективности системы защиты информации. Наиболее эффективным способом решения данной задачи является аудит информационной безопасности. Аудит информационной безопасности также относится к мерам защиты информации на объекте информатизации ОВД.

Аудит информационной безопасности (аудит ИБ) — это систематическое, независимое исследование и оценка информационных систем, процессов и политик организации с целью выявления уязвимостей, рисков и несоответствий стандартам безопасности.

Целями работ по аудиту состояния информационной безопасности АС исполнительных органов государственной власти и органов местного самоуправления субъектов России являются:

– получение объективной и независимой оценки текущего состояния защищенности информационных ресурсов и эффективности существующих систем информационной безопасности;

– повышение уровня надежности и информационной безопасности АС ИОГВ и ОМС до достаточного уровня;

– обеспечение соответствия системы информационной безопасности ИОГВ и ОМС обязательным требованиям и рекомендациям нормативно-правовых документов;

– получение максимальной отдачи от средств, инвестируемых в создание (совершенствование, модернизацию) системы информационной безопасности автоматизированных систем исполнительных органов государственной власти и органов местного самоуправления [3].

Резюмируя, главной целью аудита информационной безопасности является обеспечение надежной защиты информации и минимизация рисков утечки, утраты или несанкционированного доступа к данным.

Проведение аудита ИБ в ОВД может состоять из следующих этапов:

1) разработка плана проведения аудита ИБ в ОВД;

2) анализ документов, необходимых для проведения аудита ИБ в ОВД;

3) подготовка необходимых ресурсов для проведения аудита ИБ в ОВД;

4) проведение аудита ИБ в ОВД;

5) подготовка, утверждение и сдача отчета по аудиту ИБ в ОВД;

6) завершение процесса проведения аудита ИБ в ОВД;

7) разработка и внедрение дополнительных мероприятий по результатам аудита ИБ в ОВД.

На объекте информатизации ОВД для проведения аудита ИБ комплектуется аудиторская группа. Должен быть назначен руководитель аудиторской группы, ответственный за проведение проверки на объекте информатизации ОВД.

При определении размера и состава аудиторской группы на объекте информатизации ОВД должны быть учтены цели аудита ИБ, его масштаб и продолжительность. Должна учитываться общая компетентность и уровень квалификации аудиторской группы, а также способность членов аудиторской группы совместно работать и эффективно взаимодействовать с сотрудниками ОВД.

По результатам аудита ИБ в ОВД должны быть разработаны дополнительные мероприятия по защите информации на объекте информатизации ОВД. После проведения дополнительных мероприятий их результативность должна проверяться путем проведения очередного аудита ИБ в ОВД [4].

Достаточно давно возникла необходимость в разработке единого подхода в области обеспечения аудита ИБ. В настоящий момент в России в целом, соответственно и в МВД, нет нормативно-правового обеспечения для проведения аудита ИБ. Аудит ИБ не проводится повсеместно в органах внутренних дел, исключением служит аудит отдельных информационных технологий и систем. В связи с этим информационная безопасность органов внутренних дел не близка к совершенству. Защита информации в ОВД осуществляется в соответствии с нормами, предписывающими, в основном, только техническую защиту, путем использования моделей нарушителей. Гораздо эффективнее защита информации, основанная на анализе рисков, уязвимостей и угроз информационной безопасности, которые, как раз, и выясняются при проведении аудита ИБ.

Нормативно-правовую базу можно создать, взяв за основу уже имеющиеся нормативные документы. Например, в Федеральном законе «Об аудиторской деятельности» отмечены общие положения проведения аудита, в основном это применимо к финансовой деятельности, но может стать и фундаментом нормативного обеспечения аудиторской деятельности в области информационной безопасности. Существуют также международные стандарты, которые могут стать полезны при решении вопроса нормативного обеспечения аудита ИБ.

Еще одной проблемой проведения аудита ИБ в ОВД является использование иностранного программного и инструментального обеспечения. В данной области тоже остро чувствуется необходимость импортозамещения в целях повышения информационной безопасности.

Таким образом, объекты информатизации ОВД нуждаются в качественном обеспечении информационной безопасности, так как хранят информацию, распространение которой может нанести ущерб как отдельному гражданину, так и государству в целом. Для этого необходимо создавать комплексную систему защиты информации на объекте информатизации ОВД, которая будет включать как эффективные организационные меры защиты, так и сертифицированные средства защиты информации. Кроме того, необходимо планово и

систематически проводить аудит ИБ в каждом органе внутренних дел, а для эффективного проведения аудита — создать нормативно-правовое обеспечение аудиторской деятельности в области информационной безопасности как на ведомственном уровне, так и на уровне всей страны.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200057516 (дата обращения: 03.10.2023).
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Доступ из справочно-правовой системы «Консультант-плюс».
3. Аудит информационной безопасности органов исполнительной власти: учебное пособие для высшего образования / В. Т. Еременко [и др.]. Орел : ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», 2016. 93 с.
4. Козьминых С. И., Козьминых П. С. Аудит информационной безопасности // Вестник Московского университета МВД России. 2016. № 1. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/audit-informatsionnoy-bezopasnosti (дата обращения: 04.10.2023).
5. Федеральный закон от 30.12.2008 № 307-ФЗ «Об аудиторской деятельности». Доступ из справочно-правовой системы «Консультант-плюс».

УДК 510.65; 699.8

ПРАВОВОЕ ОБОСНОВАНИЕ РОЛИ И МЕСТА ПОЖАРНОЙ БЕЗОПАСНОСТИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Синещук Юрий Иванович, Терёхин Сергей Николаевич, Шидловский Григорий Леонидович
Санкт-Петербургский университет ГПС МЧС России
Московский пр., 149, Санкт-Петербург, 196105, Россия
e-mails: sinegal53@mail.ru, expert_terehin@igps.ru, shidlovsky.g@igps.ru

Аннотация. Определяется правовая основа обеспечения безопасности государства. Рассматриваются единые субъекты и объекты обеспечения безопасности от различных угроз. Обосновывается возможность и закономерность рассмотрения пожарной безопасности как системообразующего элемента национальной безопасности, наряду с информационной безопасностью.

Ключевые слова: национальная безопасность, информационная безопасность, пожарная безопасность.

LEGAL JUSTIFICATION OF THE ROLE AND PLACE OF FIRE SAFETY IN ENSURING INFORMATION SECURITY

Sineshchuk Yury, Terehin Sergey, Shidlovsky Grigory
Saint-Petersburg university of State fire service of EMERCOM of Russia
149 Moskovskiy Av, St. Petersburg, 196105, Russia
e-mails: sinegal53@mail.ru, expert_terehin@igps.ru, shidlovsky.g@igps.ru

Abstract. The legal basis for ensuring the security of the state is determined. Unified subjects and objects of security against various threats are considered. The possibility and regularity of considering fire safety as a system-forming element of national security, along with information security, is substantiated.

Keywords: national security, information security, fire safety.

Правовую основу обеспечения безопасности составляют Конституция РФ, общепризнанные принципы и нормы международного права, международные договоры РФ, федеральные конституционные законы, настоящий Федеральный закон, другие федеральные законы и иные нормативные правовые акты РФ, законы и иные нормативные правовые акты субъектов РФ, органов местного самоуправления, принятые в пределах их компетенции в области безопасности. Из содержания статьи 20 Конституции России вытекает, что право на жизнь содержит в своем нормативном содержании фундаментальное право на безопасность. Это предполагает обязанность государства по созданию целостной системы национальной безопасности, защиты личности от различных угроз, внутренних и внешних. Конкретизируют национальную безопасность (сочетающую в своем содержании различные виды безопасности, в том числе военную, экономическую, информационную и др.) целый ряд нормативных правовых актов, посвященных регулированию ее обеспечения: федеральный закон «О безопасности», Стратегия национальной безопасности РФ, «Доктрина информационной безопасности» и многие другие [1].

Закон РФ ФЗ № 390 «О безопасности» определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством РФ. «Доктрина информационной безопасности» определяет, что единым объектом защиты являются сбалансированные интересы личности, общества и государства в обеспечении информационной безопасности. Вместе с тем, ФЗ № 69 «О пожарной безопасности» определяет, что «пожарная безопасность — состояние защищенности личности, имущества, общества и государства от пожаров» [2].

Анализ показывает, что при реализации интересов общих субъектов безопасности выявляются и общие материальные объекты, подлежащие защите. К ним относятся: помещения; объекты инфраструктуры, средства информатизации и, конечно, люди. В процедурном аспекте это определяет необходимость организации физической защиты этих объектов от различного рода угроз, под которыми понимается совокупность действий и факторов, создающих опасность нанесения ущерба. Существенной угрозой для защищаемых объектов

являются пожары, которые представляют собой высоко опасные общественные явления, противодействие которым является одной из главных задач государства в сфере обеспечения национальной безопасности. Таким образом, пожарную безопасность можно, вполне закономерно и обосновано, рассматривать как структурный элемент (вид) национальной безопасности [3, 4]. А учитывая подверженность угрозам возникновения пожаров практически всех сфер жизнедеятельности государства, пожарную безопасность следует позиционировать, как системообразующий элемент, наряду с информационной безопасностью, в отношении которой пожарную безопасность можно рассматривать как своеобразную физическую платформу, от качества обеспечения которой зависит возможность реализации всех других видов национальной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Капранова Ю. В., Овсепян Г. М. Пожарная безопасность в системе национальной безопасности: отдельные аспекты законодательного регулирования // Юрисконсульт в строительстве. 2021. № 12. С. 38-42.
2. Рукин М. В. Пожарная безопасность объектов хранения цифровой электронной информации: центров обработки данных (ЦОД), электронных библиотек, серверных. [Электронный ресурс]. URL: https://ervist.ru/support/publikatsii/item/317-.htm (дата обращения: 01.10.2023).
3. Kotenko I., Sineshchuk Y., Saenko I. Optimizing secure information interaction in distributed computing systems by the sequential concessions method // 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP. 2020. № 28. Pp. 429-432.
4. Синещук Ю. И., Терехин С. Н. Роль и значение информационных технологий и систем в профессиональной деятельности сотрудников МЧС России // Проблемы управления рисками в техносфере. 2017. № 1 (41). С. 119-127.

УДК 510.65; 699.8

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ ПРЕДУПРЕЖДЕНИЯ КОРРУПЦИОННЫХ ПРЕСТУПЛЕНИЙ

Синещук Юрий Иванович[1], Локнов Алексей Игоревич[2]
[1]Санкт-Петербургский университет ГПС МЧС России
Московский пр., 149, Санкт-Петербург, 196105, Россия
[2] Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1 Санкт-Петербург, 198206, Россия
e-mails: sinegal53@mail.ru, info_for_aleksey@mail.ru

Аннотация. Определяется роль методов защиты информации в деятельности по предупреждению коррупционных преступлений. Рассматриваются задачи средств защиты информации в противодействии коррупции и обосновывается перечень их решений.

Ключевые слова: информатизация, информационные технологии, коррупция, защита информации.

METHODS OF INFORMATION PROTECTION IN THE SYSTEM OF PREVENTION OF CORRUPTION CRIMES

Sineshchuk Yury[1], Loknov Aleksey[2]
[1] Saint-Petersburg university of State fire service of EMERCOM of Russia
149 Moskovskiy Av, St. Petersburg, 196105, Russia
[2] St. Petersburg University of the Ministry of Internal Affairs of the Russian Federation
1 Letchika Piljutova street, St. Petersburg, 198206, Russia
e-mails: sinegal53@mail.ru, info_for_aleksey@mail.ru

Abstract. The role of information protection methods in the prevention of corruption crimes is determined. The tasks of information security tools in combating corruption are considered and a list of their solutions is substantiated.

Keywords: informatization, information technology, corruption, information protection.

Необходимость анализа возможностей предупреждения коррупционных преступлений посредством методов защиты информации (ЗИ) вызвана прежде всего условиями стремительно развивающейся информатизации, внедрением современных информационных систем, которые, в свою очередь, закономерно влекут неправомерное злоупотребление новыми возможностями высоких технологий, в том числе для совершения преступлений криминального, террористического, коррупционного характера. Коррупционное действие предполагает получение дополнительного дохода должностным лицом вследствие злоупотребления своими должностными правами и полномочиями. Возможности таких действий приобретают новый характер в современном информационном обществе, где информация образует важнейший элемент его жизнедеятельности и обретает реальную ценность [1]. Коррупционные действия в информационной сфере предполагают возможность реализации различного рода манипуляций с информацией, представляющей интерес для определенного круга лиц, доступ к которой имеет коррупционер. Развитие технологий приводит к формированию новой цифровой реальности, и может порождать новые коррупционные схемы, что в итоге приводит к электронной коррупции. Вместе с тем, именно век информационных технологий, цифровизации и автоматизации дает возможность применить новые методы в борьбе с коррумпированностью некоторых социальных групп общества. Это обусловливает актуальность применения методов обеспечения ЗИ в комплексной системе мер предупреждения коррупционных преступлений. В аспекте ЗИ важнейшим направлением деятельности становится не просто ЗИ, но и контроль правомочности доступа и манипулирования информацией, как одно из важных средств выявления коррупционных действий [2].

Методы и средства ЗИ можно использовать в сфере борьбы с коррупцией в форме противодействия такого рода правонарушениям путем их выявления, анализа, расследования и мониторинга рисков их совершения. К комплексу решений в сфере ЗИ, позволяющих выполнить указанные функции, можно отнести: управление привилегированными пользователями(Privileged User Management, PUM), предотвращение утечек информации (Data Leak Prevention, DLP), мониторинг продуктивности и работы сотрудников (Employee Monitoring Tools, EM Tools), корпоративное управление безопасностью паролей (Enterprise Password Manager, EPM), управление учетными записями и правами доступа (Identity & Access Governance, IAG), управление информацией о безопасности и событиями безопасности (Security Information & Event Management, SIEM), корпоративные межсетевые экраны (Enterprise Network Firewall, ENFW), терминальный сервер (Terminal Server), управление доменными групповыми политиками (Domain Group Policy Management, GPM) [3].

СПИСОК ЛИТЕРАТУРЫ

1. Кравченко А. Г., Овчинников А. И., Мамычев А. Ю., Воронцов С. А. Использование цифровых технологий в сфере противодействия коррупции // Административное и муниципальное право. 2020. № 6. С. 52–63
2. Ханахмедова И. А., Калинкина А. А., Южиков А. А. Технологии и методы противодействия коррупции с применением информационных технологий // Современные научные исследования и инновации. 2020. № 11 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2020/11/93752 (дата обращения: 01.10.2023).
3. Kotenko I., Saenko I., Sineshchuk Yu., Kuvatov V., Chudakov O. Optimization of the cyber security system structure based on accounting of the prevented damage cost // Proceedings of ACM 12th International Conference on Security of Information and Net-works, Sochi, Russia, September 2019 (SIN 2019). № 7. Pp. 1–8. https://doi.org/10.1145/3357613.3357620.

УДК 021

ИНФОРМАТИЗАЦИЯ БИБЛИОТЕК КАК КЛЮЧЕВОЕ НАПРАВЛЕНИЕ ГОСУДАРСТВЕННОЙ БИБЛИОТЕЧНОЙ ПОЛИТИКИ РОССИИ

Стахно Роман Евгеньевич
Санкт-Петербургский университет МВД, России
Летчика Пилютова ул.. 1, Санкт-Петербург, 198206. Россия
e-mail: piter_rus@mail.ru.ru

Аннотация. Рассмотрены организационные проблемы недостаточных темпов информатизации библиотек и неудовлетворительного состояния их материальной базы. Главной задачей государственной библиотечной политики является модернизация библиотек на основе информационных технологий в русле общемировых тенденций развития информационного общества, что позволяет ослабить негативный фактор нарастающих региональных различий в уровне библиотечного обслуживания населения и ресурсного обеспечения библиотек России.

Ключевые слова: библиотечная информация, технические средства, электронная информация, документы, обмен информацией.

INFORMATIZATION OF LIBRARIES AS A KEY DIRECTION OF THE STATE LIBRARY POLICY OF RUSSIA

Sakhno Roman
St. Petersburg University of the Ministry of internal Affairs, Russia
1 Pilot Pilyutova, St.., St. Petersburg, 198206. Russia
e-mail: piter_rus@mail.ru.ru

Abstract: The organizational problems of insufficient rates of informatization of libraries and the unsatisfactory state of their material base are considered. The main task of the state library policy is the modernization of libraries based on information technologies in line with the global trends in the development of the information society, which makes it possible to weaken the negative factor of the growing regional differences in the level of library services to the population and the resource provision of libraries in Russia.

Keywords: library information, technical means, electronic information, documents, information exchange.

Библиотечная информация представляет собой совокупность документированных сведений, являющихся объектом сбора, хранения, создания (преобразования) и предоставления (распространения) в процессе осуществления библиотечно-информационной деятельности, а также сведений о библиотеке и (или) документированной библиотечной информации.

Библиотечная информация находит свое материальное воплощение в форме информационных ресурсов, которые в библиотековедении рассматриваются как запасы информации, зафиксированной на каком-либо носителе и пригодной для ее сохранения и использования.

Объектом информационных правоотношений также выступает библиотечный фонд. Библиотечный фонд является хранилищем первичных документных библиотечно-информационных ресурсов. ГОСТ Р 7.0.97—2016 «Система стандартов по информации, библиотечному и издательскому делу» относит к объектам комплектования библиотечного фонда: опубликованный документ, неопубликованный документ, обязательный экземпляр документов, информационные ресурсы, под которыми понимается совокупность данных,

организованных для эффективного получения достоверной информации, а также электронный ресурс. Важно отметить, что вопрос об отнесении сетевых ресурсов удаленного (дистанционного) доступа к объектам библиотечного фонда является на данный момент дискуссионным.

Целями организации электронных библиотек являются:

– предоставление пользователям качественно новых возможностей работы с большими объемами машиночитаемых данных;

– обеспечение доступа пользователей к электронной информации локального и удаленного уровня;

– целенаправленное создание уникальных электронных информационных массивов [1].

Основная задача электронных библиотек заключается в интеграции электронных ресурсов и организации эффективной навигации в них. К основным особенностям электронных библиотек следует отнести:

– инвентаризацию, в частности каталогизацию, объектов и различных их объединений, которые образуют это информационное пространство;

– профильность хранимой информации, то есть наличие определенной концепции формирования информационного пространства, доступного пользователю, и политика ее реализации.

Фундаментом, основой, которая объединяет традиционные и электронные библиотеки, является принцип обслуживания пользователей.

Важной составляющей любой электронной библиотеки является ее электронный каталог [2].

Электронный каталог — в отличие от каталога на бумажных носителях (систематический и алфавитный), его целью является обеспечение расширенного перечня критериев поиска информации.

Например, в обычном классическом каталоге читатель может осуществлять поиск только по алфавиту авторов (алфавитный каталог) либо по тематике необходимой литературы (систематический каталог). В электронном же каталоге помимо основных критериев, читатель может указывать и дополнительные.

Передавая информацию, библиотеки зачастую сталкиваются с необходимостью критического отбора содержания находящихся в фонде материалов. В отличие, например, от сети Интернет, в которой содержится масса почти никак не систематизированной информации. Использование такой информации требует высокой квалификации, которой читатель не всегда владеет.

Как информационные центры библиотеки должны осуществлять предварительный отбор, грамотную систематизацию и осмысление передаваемой информации.

Достаточно остро стоит в это время и проблема обеспечения сохранности библиотечных фондов. Печатные материалы быстро изнашиваются. Однако в современный период начинается процесс оцифровки наиболее ценных документов.

Напрямую с проблемой сохранности и неудовлетворенности читательских запросов связана проблема недостаточных темпов информатизации библиотек и неудовлетворительного состояния их материальной базы. Процесс компьютеризации с одной стороны тормозился хронической нехваткой финансирования, с другой — низкой компьютерной грамотностью населения и работников библиотек.

В переходный период, главной задачей государственной библиотечной политики является модернизация библиотек на основе информационных технологий в русле общемировых тенденций развития информационного общества, что позволяет ослабить негативный фактор нарастающих региональных различий в уровне библиотечного обслуживания населения и ресурсного обеспечения библиотек России.

Информатизация библиотек имеет значительные преимущества:

– применение технических средств в сфере библиотечного обслуживания способствует расширению сферы обслуживания библиотек. Это влияет на увеличение объёма, предоставляемой информации;

– создание электронных каталогов намного упрощает поиск информации [3];

– электронные информационные хранилища постепенно заменяют реальные библиотеки. Постепенно уменьшается количество офлайн заведений. Благодаря этому экономятся важные ресурсы;

– быстрый обмен информацией обеспечивает эффективную коммуникацию как между отдельными библиотеками, так и между библиотекой и пользователем библиотек;

– сохранность определенных экземпляров. Возможность создания большого количества электронных копий, что обеспечивает сохранность информации. Все же бумажные носители недолговечны, большое количество бумажных экземпляров, особенно при нарушении правил хранения книг, обретают физические дефекты. Также бумажные экземпляры могут быть просто утеряны;

– популяризацию библиотек тоже можно отнести к преимуществам информатизации библиотек. Ведь при создании электронных библиотек доступ к информации упрощается. Это фактор привлекает людей становиться пользователями библиотек.

Информатизация библиотек имеет огромное значение в процессе формирования глобального информационного общества.

СПИСОК ЛИТЕРАТУРЫ

1. Литвинова Н. Н. Лицензии на доступ к сетевым удаленным ресурсам: продолжение темы // Науч. и техн. б-ки. 2017. № 6.
2. Редькина Н. С. Службы информационных технологий в научных библиотеках // Науч. и техн. б-ки. 2016. № 11.
3. Базовые информационно-коммуникационные технологии : учебно-метод. пособие для студентов по спец. 351400 «Прикладная информатика» / сост. О. И. Волков, Р. К. Камалетдинов. Казань : КГУКИ, 2017. 56 с.

УДК 004.056:51

ИНФОРМАЦОННО-АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ В ВОЕННОМ ДЕЛЕ

Шалагинова Ольга Борисовна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: shalaginova1337@yandex.ru

Аннотация. В данной статье отмечается, что в последние годы МВД России совершенствует информационно-аналитическое обеспечение оперативно-служебной деятельности полиции. Внедрены типовые программные решения по интеграции данных, по организации единого информационного пространства в системе МВД России; категорированы основные подходы и определены уровни формирования информационных массивов в субъектах федерации и в стране в целом.

Ключевые слова: информационная безопасность; информационные пространства; управленческое реагирование; геоинформационное обеспечение; цифровые модели.

INFORMATION AND ANALYTICAL SUPPORT IN MILITARY AFFAIRS

Shalaginova Olga Borisovna
St. Petersburg University of the Ministry of Internal Affairs of Russia
1 Pilot Pilyutova str., St. Petersburg, 198206, Russia
e-mail: shalaginova1337@yandex.ru

Abstract. This article notes that in recent years, the Ministry of Internal Affairs of Russia has been improving information and analytical support for operational and service activities of the police. Standard software solutions for data integration, for the organization of a single information space in the system of the Ministry of Internal Affairs of Russia have been introduced; the main approaches have been categorized and the levels of formation of information arrays in the subjects of the federation and in the country as a whole have been determined.

Keywords: information security; information spaces; management response; geoinformation support; digital models.

С развитием современного общества и появлением новых технологий, число рабочих мест в области информационной безопасности растет высокими темпами. Поэтому с таким образованием очень трудно остаться без работы, ведь число востребованных специалистов очень высоко. Причем работать можно не только в отдельных компаниях и частных предприятиях, но также выпускники смогут пойти на службу в МВД, следственные комитет, прокуратуру, и другие государственные объекты. Все это гарантирует специалисту высокую заработную плату, а также престижный статус сотрудника. Тем более, выплаты в этом направлении деятельности регулярно растут, так как система постоянно развивается и укрепляется. В среднем, доход рядового специалиста на начальных этапах составляет от 60 тысяч рублей и выше.

Приводятся различные признаки и угрозообразующие факторы, которые могут свидетельствовать о возможных правонарушениях и преступлениях, связанных с коррупцией, рейдерскими захватами предприятий, работой промышленных предприятий, инвестиционно-строительных корпораций, а также деятельностью в сфере электронного бизнеса.

Следует отметить, что в последние годы МВД России системно совершенствует информационно-аналитическое обеспечение оперативно-служебной деятельности полиции. На данный момент проделана большая работа по внедрению в эту деятельность различных современных автоматизированных информационных систем и программно-технических комплексов [1]. В частности, внедрены типовые программные решения по интеграции данных; предприняты шаги по организации единого информационного пространства в системе МВД России; категорированы основные подходы и определены уровни формирования информационных массивов в субъектах федерации и в стране в целом. Все это позволило упорядочить и системно организовать все основные связи между подразделениями федерального, регионального и районного звеньев ОВД, а также оптимизировать уровни доступа и порядок сбора информации, определить рациональный состав оборудования, информационных, технико-технологических и других ресурсов [2]. Под информационной безопасностью органов внутренних дел понимается их защищенность от случайного или преднамеренного вмешательства в нормальный процесс функционирования, а также попыток хищения, изменения или разрушения ее компонентов. Информационная безопасность органов внутренних дел достигается принятием мер по обеспечению конфиденциальности информации, а также доступности и целостности ее компонентов и ресурсов.

Что касается информационного обеспечения современных вооруженных сил [3], то хотелось бы коснуться научно-практических перспектив развития такой важной для безопасности государства сферы, как топогеодезическое и навигационное обеспечение. Несмотря на то, что сегодня при стратегическом, тактическом и оперативном управлении войсками используются классические топографические карты, после динамичного роста масштабности и скоротечности современных военных операций и кардинального обновления разновидностей видов и средств вооружения соответственно расширилась и номенклатура носителей топогеодезической информации. Основной задачей данных носителей является предоставление оперативной объективной информации. Осуществляется это с помощью генерации и фильтрации больших объемов гетерогенных данных,

путем использования разных направлений технического прогресса: систем распознания фото- и видеоизображений или речи, нейронных и семантических сетей и использования возможностей «искусственного интеллекта». Аспекты точности и оперативности получения информационных и геоданных о территориях, находящихся в зоне боевых действий или подконтрольных и сопредельных территориях, при динамичном управлении войсками становятся ключевым звеном для принятия решений и контроля командованием вооруженных сил.

Быстротечность современных вооруженных столкновений требует разработки и внедрения в военное дело все большего числа механизмов и инструментов, позволяющих оптимизировать развертывание воинских подразделений и гибкое управленческое реагирование при своевременной коррекции информации о действиях противника. Поэтому задача формирования целостного информационно-коммуникационного пространства с помощью информационных технологий является основой положительного результата при столкновении или противостоянии, за счет предоставления своевременной и объективной картины боевой обстановки и динамики ее изменений. Тем самым достигается опережение противостоящей стороны в сборе и анализе информации, принятии стратегических и тактических командных решений и оперативном доведении их до воинских подразделений, участвующих в конфликте. Благодаря появлению более совершенных носителей цифровой аудио- и видеосвязи, топогеодезическое обеспечение вооруженных сил XXI в., включающее аэрокосмическую, оптико-электронную разведку с применением цифровой компьютерной обработки, стало основой передачи информации в современной армии. Основой же геоинформационного обеспечения является использование каналов, связанных с базами данных географических информационных систем с целью планомерной циркуляции оперативных данных для передачи географической или топографической информации в цифровой форме. Таким образом, формируются информационные базы данных и цифровые карты местности с целью всестороннего отражения сведений для электронной визуализации и возможности интерактивной работы пользователя. При этом современные технологии позволяют создавать и поддерживать цифровые модели оперативной обстановки для каждого конкретного задания с учетом специфики конкретной военной структуры.

СПИСОК ЛИТЕРАУРЫ

1. Берестень В. И., Берестень А. В. Информационно-аналитическая деятельность в интересах обеспечения национальной безопасности в военной сфере // Труд. Профсоюзы. Общество : журнал. 2022. № 2 (76). С. 39-45.
2. Иванов А. А., Кудрявцев А. М., Смирнов А. А. Концептуальные проблемы информационно-аналитической работы в современном военном противостоянии // Военная мысль. 2020. № 9. С. 79.
3. Артеменко В. Б., Безденежных И. В., Василецкий Ю. Л. Система военно-научной информации вооруженных сил российской федерации: вчера, сегодня, завтра // Вооружение и экономика. 2022. № 3 (61). С. 143-158.

УДК 343.973

МАТЕМАТИКА В БОРЬБЕ С ПРЕСТУПНОСТЬЮ

Шалагинова Ольга Борисовна
Санкт-Петербургский университет МВД России,
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: shalaginova1337@yandex.ru

Аннотация. В данной статье отмечается особая актуальность математических методов, формул и алгоритмов в деятельности ОВД. Это неотъемлемая часть таких методов, используемых для раскрытия преступлений, как снятие отпечатков пальцев, воспроизведение событий дорожных происшествий, фиксация автомобильных номерных знаков, а также отслеживание маршрутов преступников.

Ключевые слова: математические методы; анализ данных; моделирование; обратные задачи; следствие.

MATHEMATICS IN THE FIGHT AGAINST CRIME

Shalaginova Olga
St. Petersburg University of the Ministry of Internal Affairs of Russia,
1 Pilot Pilyutova str., St. Petersburg, 198206, Russia
e-mail: shalaginova1337@yandex.ru

Abstract. This article notes the special relevance of mathematical methods, formulas and algorithms in the activities of the Department of Internal Affairs. This is an integral part of such methods used to solve crimes as fingerprinting, reproducing road accidents, fixing car license plates, as well as tracking the routes of criminals.

Keywords: mathematical methods; data analysis; modeling; inverse problems; consequence.

Борьба с преступностью — возможно, не самая первая мысль, которая приходит на ум, когда думаешь о математике. Задайте вопрос кому-нибудь на улице, как они думают о математике, и, к сожалению, их ответ вполне может быть: «Математику изучают только в школе». Но на самом деле, математические методы, формулы и алгоритмы очень актуальны в деятельности ОВД [1]. Это неотъемлемая часть многих методов, используемых полицией для раскрытия преступлений, в том числе при снятии отпечатков пальцев, воспроизведении событий дорожных происшествий, фиксации автомобильных номерных знаков, а также отслеживании маршрутов преступников.

Правоохранительные органы сталкиваются с множеством проблем при борьбе с преступностью. Сотрудникам необходимо в кратчайшие сроки выяснить, что произошло на месте преступления или происшествия, разыскать и найти преступников, предъявить доказательства их вины. Для этого им необходимо получать достоверную информацию, которую они смогут применять в ходе выяснения обстоятельств дела. И, в интересах правосудия, доказательства, как материальные, так и электронные, должны обязательно храниться в безопасности.

Математика может помочь с этими задачами. Например, анализ данных, полученных в ходе оперативно-розыскных мероприятий, следственных действий, судебных экспертиз с использованием методов теории вероятностей или статистики [2]. Также любые сведения можно безопасно обрабатывать и передавать с помощью простых чисел и криптографии [3]. Но, прежде всего, полиции нужно получить информацию, лежащую в основе данных. Сотрудники должны внимательно осмотреть все улики, оставленные на месте преступления. А для того, чтобы было легче установить, что произошло, и кто совершил преступление, работать стоит в обратном направлении. Часто улики являются результатом хорошо изученного физического процесса, например, когда автомобиль едет с большой скоростью, он оставляет следы заноса на дороге. Итак, чтобы выяснить точную причину свидетельства — высокой скорости автомобиля — необходимо выполнить в обратном порядке математические вычисления, описывающие физику движения транспортного средства. Это называется решением обратной задачи. Разобрать её можно с помощью нескольких примеров.

Обратные задачи — это математические детективные задачи. Примером обратной задачи может считаться попытка найти объект, зная только форму его тени. Возможно ли это вообще? Какие ошибки можно совершить, и сколько дополнительной информации потребуется?

Чтобы решить обратную задачу, нужна физическая модель события — нужно понять, какие причины приводят к тем или иным последствиям. Затем, учитывая известные результаты, можно использовать математические методы, чтобы определить возможные причины, например, определить, какие объекты и какой формы отбрасывают именно такую тень на анализируемой фотографии. Также математику используется в ситуациях, когда нужно установить ограничения модели и точность ответа. В примере с тенями, отбрасываемыми объектами, существуют разные причины: разные объекты пусть похожей формы могут отбрасывать одинаковые тени.

Имеющиеся доказательства — это повреждения транспортных средств в результате столкновения, показания свидетелей и следы заноса шин. Анализ следов заноса может помочь восстановить картину аварии. Следы вызваны превышением допустимой скорости автомобилем, а также другими факторами, такими как: тормозное усилие, трение с дорогой и столкновение с другим транспортным средством.

С точки зрения математики можно рассмотреть механику движения автомобиля для моделирования этого события, при этом используются различные полученные данные: длина заноса, скорость транспортного средства, ускорение свободного падения и коэффициент трения, умноженный на эффективность торможения. Модель связывает причину-скорость автомобиля со следствием — расстояние заноса. Решается задача так, что, зная расстояние пути скольжения, можно математически определить скорость автомобиля, задав её нижнюю границу. Но для того, чтобы расчёты были верны, нужна точная оценка значения, описывающего трение и эффективность торможения.

Другими примерами обратных задач являются: дистанционное зонирование суши или моря по спутниковым изображениям, использование медицинских изображений для диагностики опухолей и интерпретация сейсмографов для поиска нефти.

СПИСОК ЛИТЕРАТУРЫ

1. Авраменко А. А., Хмелёва А. А., Крапивина Л. А. Математика в различных профессиях // Международный студенческий научный вестник. 2020. № 2. С. 141.
2. Туробов А. В., Чумакова М. А., Вечерин А. В. Международный опыт применения математико-статистических алгоритмов прогнозирования преступности // Международные процессы. 2019. № 17 (4). С. 153-177.
3. Хатов Э. Б. О роли цифровых технологий в анализе преступности // I Всероссийская научно-практическая конференция «Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции (Долговские чтения)». 2021. С. 41-47.

УДК 004

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО БЛАГОПОЛУЧИЯ ЛИЧНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Шилков Владимир Ильич
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина,
Мира ул., 19, Екатеринбург, 620002, Россия
e-mail: shilkov-urfu@yandex.ru

Аннотация. Обсуждаются правовые аспекты и проблемы, связанные с деструктивным информационно-психологическим воздействием на информационную безопасность и благополучие личности. Декларируется необходимость: периодической актуализации правовой терминологии в сфере анализа информационной безопасности личности; применения методов системного подхода и консолидации усилий различных специалистов. Обозначена необходимость решения правовых проблем в целях создания международного правового и безопасного информационного пространства.

Ключевые слова: информационная безопасность, благополучие личности, информационное пространство.

LEGAL ASPECTS OF INFORMATION AND PSYCHOLOGICAL WELL-BEING OF THE INDIVIDUAL IN THE CONTEXT OF DIGITAL TRANSFORMATION

Shilkov Vladimir
Ural Federal University, named after the First President of Russia B. N. Yeltsin,
19 Mira St., Yekaterinburg, 620002, Russia
e-mail: shilkov-urfu@yandex.ru

Abstract. Legal aspects and problems related to the destructive informational and psychological impact on information security and well-being of the individual are discussed. The necessity is declared: periodic updating of legal terminology in the field of personal information security analysis; application of methods of a systematic approach and consolidation of efforts of various specialists. The necessity of solving legal problems in order to create an international legal and secure information space is indicated.

Keywords: information security, personal well-being, information space.

Цифровая трансформация мировой системы социально-экономических отношений привела к возникновению целого ряда неотложных проблем, связанных негативным действием информационных факторов. Одной из актуальных проблем существенных для благополучия отдельной личности, государства и всего мирового сообщества стала проблема противоправного деструктивного информационного воздействия. Данную проблему, имеющую комплексный характер необходимо решать с учетом правовых, технических, социально-экономических и психологических аспектов, возникших в связи с появлением глобального информационного пространства.

Для решения задачи минимизации деструктивного влияния негативных факторов цифровой трансформации на личностное и общественное благополучие необходимо применение методов системного подхода и консолидация усилий многих специалистов: юристов, социологов, психологов, экономистов и специалистов по информационной безопасности. Комплексный характер данной задачи делает необходимым постоянное сопровождение и актуализацию правовых, психологических и технологических аспектов особенностей информационной безопасности и благополучия личности и государства.

Актуальными являются вопросы разработки моделей мотивации, психологических портретов злоумышленников и потенциальных жертв, информационных угроз и методов противодействия информационно-деструктивному влиянию. Злоумышленники, используя возможности средств массовых коммуникаций и динамично развивающихся современных информационно-коммуникационных технологий (ИКТ), могут вовлекать людей в авантюрные экономические проекты, в социально-опасную деятельность, распространять идеи экстремистского характера, формировать массовую культуру, манипулировать социальными проблемами и потребностями населения, навязывая собственные интересы и оказывая деструктивное воздействие в масштабах регионального, национального и глобального информационного пространства [1].

С помощью систем информационных фильтров злоумышленники могут управлять информационными потоками, навязывая широкой аудитории свои собственные способы решения психологических, экономических проблем, стандарты поведения и модели восприятия окружающей действительности [2].

Одной из современных форм деструктивного информационного воздействия на личность являются, так называемые, фейковые новости, распространяемые под видом достоверного контента и содержащие в себе общественно-значимую, но не соответствующую действительности, информацию. Злоумышленники, осуществляющие вброс фейковой информации, которая в своей формулировке, часто допускает неоднозначное толкование, не подтверждая или не опровергая какой-либо реальный факт, могут преследовать различные цели. Фейковая информация, воздействуя на подсознание и психику личности, как правило, способствует созданию обстановки беспокойства, сомнения и неуверенности и, которая, в свою очередь, может приводить к возникновению угроз массового нарушения общественного порядка. Фейковые новости также могут быть направлены на подрыв авторитета сотрудников госслужбы или на нанесение ущерба репутации конкретной личности, что может приводить к созданию угроз их здоровью и жизни [3].

Вместе с тем, в условиях цифровой трансформации сферы социально-экономических отношений, правовая неопределенность, обусловленная инновационным характером и скоростью происходящих изменений; нерешенность правовых вопросов, связанных с межгосударственным регулированием информационных процессов в глобальном информационно-экономическом пространстве; анонимность участников, активно формирующихся неуправляемых и неконтролируемых теневых цифровых рынков; привели к появлению новых проблем и формированию благоприятных условий для возникновения и процветания новых видов противоправной деятельности.

По мнению ряда авторов, несмотря на успешное формирование законодательной концептуальной основы российского информационного суверенитета, законодательные инициативы, связанные с обеспечением защищенности, устойчивости, стабильности и целостности национального информационного пространства в ряде случаев носят разрозненный характер, не имеют легитимного закрепления и нуждаются в дальнейшей доработке. Так, например, детальная классификации преступлений в сфере информационных технологий должна осуществляться как с учетом результата анализа тенденций развития современной преступности, так и новых квалификационных признаков преступлений по каждой статье уголовного кодекса [4].

В периодическом уточнении, дополнении, разрешении ряда проблемных моментов, связанных с терминологией, содержанием и определением их правого статуса, нуждается и целый ряд терминов, применяемых в сфере современных информационно-коммуникационных технологий и необходимых для проведения комплексного экспертного анализа глобального информационного пространства и разработки методов противодействия вредоносным информационно-техническим и психологическим воздействиям, осуществляемым в ходе информационных взаимодействий в социальных сетях. Уточнения и новые трактовки терминов необходимо принимать во внимание также и в процессе актуализации правовой базы для установления ответственности за новые виды правонарушений в информационно-технологической сфере.

К терминам, нуждающимся в периодическом уточнении, следует отнести понятия «цифровая среда», «вредоносное информационное воздействие», «информационная безопасность личности», «фейковая информация». Компонентами «цифровой среды» являются информационные технологии, системы и ресурсы, участвующие в обработке цифровую информации, окружающие и являющиеся существенно значимыми для функционирования и развития анализируемого объекта, системы или события. Дефиницию «вредоносное информационное воздействие», в правовом аспекте, связывают с действиями, осуществляемыми в интересах определенных социально-политических и сил и оказывающими негативное деформирующее влияние на личность, общество и информационно-психологическую среду государства. Нуждается в правовом сопровождении и в уточнении также и термин «информационная безопасность личности», который часто связывают с состоянием защищенности личности от внешних и внутренних угроз, рассматривая только информационно-технологические аспекты этой проблемы, не уделяя должного внимания юридическим и смысловым компонентам данного понятия. В правовом аспекте, специфической особенностью применения информационных технологий с целями деструктивного информационного воздействия на личность является возможность злоумышленнику избегать непосредственного контакта с потенциальной жертвой. В свою очередь данное обстоятельство может приводить к авантюрным психологическим ощущениям недосягаемости и безнаказанности и способствовать расширению социальной сферы преступности.

Информационно-психологическая безопасность личности является важнейшим элементом национальной информационной безопасности, однако, следует отметить, что на уровне международно-правового сотрудничества, возникают определенные противоречия, обусловленные различными трактовками терминов «информационная безопасность» и «информационная безопасность личности» в различных государствах. Важность решения проблем правовой, экономической и информационно-психологической безопасности личности не только на национальном, но и на международном уровне, обусловлена в частности открытым характером глобального информационного пространства, в котором деструктивная информация может свободно пересекать границы государств, создавая угрозы информационно-психологическому благополучию личности.

К основным направлениям решения данной проблемы можно отнести два основных направления, одно из которых связано с созданием условий для информационной обособленности государства с эффективными барьерами от проникновения деструктивного контента, а другое с созданием единого международного правового и безопасного информационного пространства с едиными стандартами информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Богомаз О. В. Обеспечение информационной безопасности детей и молодежи: правовые, педагогические и психологические аспекты // Право. Безопасность. Чрезвычайные ситуации. 2021. № 3(52). С. 35-41.
2. Козырева А. А. Правовые аспекты формирования личной информационной безопасности в условиях деструктивного информационного воздействия // Международная гуманитарная помощь: опыт, реалии, перспективы. Актуальные вопросы формирования культуры безопасности населения (международные аспекты). XXIII Международная научно-практическая конференция по проблемам защиты населения и территорий от чрезвычайных ситуаций : материалы конференции. ФГБУ ВНИИ ГОЧС (ФЦ). 2018. С. 379-386.
3. Тюрнев А. С., Помелов А. А., Шелегов Ю. В. Обеспечение информационной безопасности: правовые аспекты проблемы // Вестник экономической безопасности. 2022. № 2. С. 169-173.
4. Дворецкий Д. А. Особенности преступлений в сфере информационных технологий в контексте информационной безопасности // Уголовно-исполнительная система: реалии и перспективы развития : материалы II Международной научно-практической конференции. Псков, 2020. С. 82-90.

УДК 004.056

СПОСОБ ОЦЕНКИ УРОВНЯ ИСХОДНОЙ ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ЛИЧНЫХ ДАННЫХ

Яковлева Наталья Александровна, Большакова Людмила Валентиновна,
Сибаров Константин Дмитриевич, Карпов Павел Евгеньевич
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: kumirova@mail.ru, blv5505@mail.ru, konstantin_siba@mail.ru, best-man82@mail.ru

Аннотация. Предлагается способ оценки уровня защищённости информационных систем личных данных с применением метода вложенных линейных свёрток.

Ключевые слова: информационная безопасность, защита персональных данных, информационные системы, линейная свёртка.

A METHOD FOR ASSESSING THE LEVEL OF INITIAL SECURITY OF PERSONAL DATA INFORMATION SYSTEMS

Yakovleva Natalia, Bolshakova Valentina, Sibarov Konstantin, Karpov Pavel
St. Petersburg University of the Ministry of Internal Affairs of Russia
1 Pilyutov's pilot St., St. Petersburg, 198206, Russia
e-mail: kumirova@mail.ru, blv5505@mail.ru, konstantin_siba@mail.ru, best-man82@mail.ru

Abstract. A method is proposed for assessing the level of security of personal data information systems using the nested linear convolution method.

Keywords: information security, personal data protection, information systems, linear convolution.

Обеспечения защиты информационных систем личных данных (ИСЛД) в настоящее время приобретает всё большее значение.

Известны следующие основные направления обеспечения защиты ИСЛД:

– Предотвращение утечки звуковой информации.

– Предотвращение утечки видовой информации.

– Предотвращение утечки информации через побочное электромагнитное излучение и наводки (ПЭМИН).

– Предотвращение несанкционированного физического доступа, уничтожения или хищения составных частей оборудования ИСЛД.

– Предотвращение несанкционированного доступа к данным с возможностью их чтения, копирования, модификации.

– Предотвращение возможностей несанкционированного изменения программной среды обработки данных.

– Предотвращение повреждений оборудования, данных и программ в составе ИСЛД вследствие непреднамеренных действий человека и природных явлений.

– Предотвращение угроз сетевой безопасности.

Каждое из этих направлений может быть охарактеризовано определённым набором количественных показателей.

Уровень обеспечения защищённости по каждому направлению можно представить в виде линейной свёртки (взвешенной суммы) его показателей. Значения показателей должны быть нормированы, т. е. принадлежать промежутку от 0 до 1, где 1 — это наилучшее значение. Весовые множители могут быть определены, например, с помощью метода экспертных оценок. Значение весового множителя тем больше, чем более важен показатель. При этом сумма всех весов должна равняться 1.

Определённый указанным образом уровень является частным, т.е. соответствующим рассматриваемому направлению обеспечения защиты ИСЛД.

Для расчёта уровня обеспечения защищённости ИСЛД по всем направлениям необходимо рассчитать обобщённый показатель. Его также можно представить в виде линейной свёртки. В ней в качестве слагаемых будут произведения частных уровней защищённости на весовые множители, отражающие относительную степень важности каждого направления.

Полученный обобщённый показатель будет принимать значения от 0 до 1, и на основе его можно будет сделать вывод о защищённости ИСЛД, например, в соответствии со следующими правилами:

0–0,25 — низкая степень;

0,25–0,50 — средняя степень;

0,5–0,75 — высокая степень;

0,75–1,0 — очень высокая степень.

СПИСОК ЛИТЕРАТУРЫ

1. Кини Р. Л., Райфа Х. Принятие решений при многих критериях: предпочтения и замещения. М. : Радио и связь, 1981.
2. Ногин В. Д. Принятие решений в многокритериальной среде: количественный подход. М. : Физматлит, 2005.
3. Петровский А. Б. Теория принятия решений. М. : Издательский центр «Академия», 2009.

УДК 004:056

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА ДЛЯ ХРАНЕНИЯ ИНФОРМАЦИИ В ДЕЯТЕЛЬНОСТИ ОВД

Якушев Денис Игоревич, Бушманов Никита Андреевич
Санкт-Петербургский университет МВД России
Лётчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: d.i.ya@yandex.ru, flash.12121@yandex.ru

Аннотация. В статье рассматривается применение распределенных реестров в работе органов внутренних дел (ОВД). Исследуются преимущества и ограничения использования этой технологии для обеспечения безопасности и эффективности работы ОВД.

Ключевые слова: Распределенные реестры, органы внутренних дел, обеспечение безопасности, информационная безопасность, хранение данных, технологии блокчейн, защита информации.

TO THE QUESTION OF USING A DISTRIBUTED REGISTRY FOR STORING INFORMATION IN THE ACTIVITIES OF THE INTERNAL AFFAIRS BODIES OF RUSSIA

Yakushev Denis, Bushmanov Nikita
Saint Petersburg University of the Ministry of internal Affairs of the Russian Federation
1 Pilyutov's pilot St., St. Petersburg, 198206, Russia
e-mails: d.i.ya@yandex.ru, flash.12121@yandex.ru

Abstract. The article discusses the use of distributed registries in the work of internal affairs bodies (ATS). The advantages and limitations of using this technology to ensure the safety and efficiency of the ATS are investigated.

Keywords: Distributed registries, internal affairs bodies, security, information security, data storage, blockchain technologies, information protection.

Современное общество стремительно развивается, и вместе с этим увеличивается поток информации, требующей хранения и обработки. Однако, помимо роста объемов информации, важно обеспечить ее надежное хранение и доступность, особенно в критических организациях, таких как органы внутренних дел (ОВД). Распределенные реестры, такие как блокчейн, предоставляют перспективное решение для обеспечения безопасности и эффективности хранения информации в ОВД.

Распределенный реестр можно использовать для записи статических данных, таких как реестр, и динамических данных, таких как финансовые транзакции.

На сегодняшний день используются различные типы технологии распределенного реестра, один из них — блокчейн.

Блокчейн — вариант реализации сети распределенных реестров, в котором данные о совершенных транзакциях структурируются в виде цепочки (последовательности) связанных блоков транзакций. Стоит отметить, что не все сети распределенных реестров функционируют на базе технологии блокчейн. Так, например, протокол Ripple подразумевает потранзакционный процессинг без формирования блоков. В случае использования блокчейн каждый новый блок транзакций подтверждается участниками сети как валидный, после чего он присоединяется (встраивается в цепочку) со всеми предыдущими операциями в распределенном реестре. Классификация сетей распределенных реестров.

Распределенные реестры: основные принципы

Распределенный реестр (distributed ledger technology, DLT) — это технологическая инновация, позволяющая создавать и поддерживать базу данных, которая распределена между несколькими участниками сети. Основной принцип распределенных реестров заключается в том, что каждый участник сети имеет копию всей базы данных, и обновления вносятся согласованно среди участников. Это обеспечивает высокую степень надежности и устойчивости к атакам и сбоям.

DLT использует криптографию для безопасного хранения данных, реализуется это с помощью механизма хэширования: распределенная база данных представляет собой цепочку последовательных специальных блоков, каждый из которых в числе прочего содержит в себе хэш предыдущего блока и свой порядковый номер. Каждый новый блок подтверждает содержащиеся в нем транзакции и дополнительно подтверждает транзакции во всех предыдущих блоках цепочки. Таким образом, достигается неизменность хранимой информации, и скорректировать информацию внутри цепи становится невозможно, не нарушив ее целостности.

Для обеспечения неизменности и подлинности транзакции используются криптографические подписи и ключи, чтобы разрешить доступ только авторизованным пользователям.

Ключевые особенности распределенного реестра:

Технология распределенного реестра имеет ряд ключевых особенностей, которые делают ее уникальной по сравнению с решениями централизованного реестра.

1. Распределенность — нет единого места, данные хранятся единовременно на всех компьютерах сети. Каждый компьютер сам отвечает за обновление и синхронизацию.

2. Необратимость записи — распределенные реестры поддерживают только добавление, поскольку они предоставляют полную историю транзакций. Это полностью отличается от традиционной базы данных, где данные могут быть изменены ради функциональности.

3. Неизменяемость — распределенный реестр использовал криптографию для создания неизменного и безопасного хранилища. Это гарантирует, что однажды сохраненные данные не могут быть изменены.

4. Алгоритм консенсуса — общая версия реестра, согласованная всеми участниками сети.

Эта архитектура представляет собой существенное изменение в способах сбора и передачи информации путем переноса ведения учета из единого авторитетного места в децентрализованную систему, в которой все соответствующие лица могут просматривать и изменять реестр. В результате все остальные лица могут видеть, кто использует и изменяет реестр. Такая прозрачность DLT обеспечивает высокий уровень доверия между участниками и практически исключает вероятность мошеннических действий в реестре.

Преимущества использования распределенных реестров для ОВД

– Безопасность данных: Распределенные реестры обеспечивают высокий уровень безопасности данных благодаря криптографии и децентрализации. Информация хранится в зашифрованной форме и не имеет единой точки отказа, что делает ее устойчивой к хакерским атакам.

– Прозрачность и целостность: Все транзакции и изменения данных в распределенном реестре регистрируются и хранятся навсегда. Это обеспечивает прозрачность и невозможность фальсификации данных.

– Снижение бюрократии: ОВД работают с большим объемом документации, и использование распределенных реестров может сократить бюрократические процедуры, ускоряя доступ к информации и облегчая ведение учета.

– Улучшение сотрудничества: Распределенные реестры позволяют нескольким сторонам совместно работать с одним источником данных без доверия к центральной стороне. Это может быть полезно для координации действий между различными отделами ОВД и другими правоохранительными органами.

– Устойчивость к сбоям: Распределенные реестры предоставляют механизмы автоматического восстановления после сбоев в сети или на устройствах участников, что обеспечивает бесперебойную работу ОВД.

Практические примеры применения

1. Учет уголовных дел: ОВД могут использовать распределенные реестры для учета уголовных дел, обеспечивая доступ к информации всем сотрудникам и избегая возможных изменений данных.

2. Регистрация имущества: Для борьбы с мошенничеством и несанкционированными изменениями в реестрах недвижимости и других имущественных правах можно использовать блокчейн-технологии.

3. Обмен информацией с другими органами: Распределенные реестры позволяют быстро и безопасно обмениваться информацией с другими правоохранительными органами, повышая эффективность совместных операций.

4. Регистрация и учет имущества и документов: Ведение цифровых реестров имущества МВД, включая автомобили, оружие и другое оборудование. Хранение электронных копий документов, связанных с деятельностью МВД, таких как протоколы, отчеты и т.д.

5. Борьба с коррупцией и злоупотреблением полномочиями: Создание системы мониторинга и аудита, позволяющей отслеживать несанкционированные изменения в данных и их историю. Усиление прозрачности и надежности ведения учета финансовых операций и расходов.

Проблемы и сложности:

Несмотря на многочисленные преимущества, существуют и вызовы при использовании распределенных реестров в ОВД. К ним относятся:

1. Проблемы конфиденциальности: Некоторая информация должна оставаться конфиденциальной, и не всегда легко обеспечить эту конфиденциальность в распределенных реестрах.

2. Сложности внедрения: Внедрение новых технологий может потребовать значительных инвестиций и времени на обучение сотрудников.

3. Законодательные аспекты: Необходимо разработать соответствующие законы и нормативы для регулирования использования распределенных реестров в правоохранительной деятельности.

Использование распределенных реестров в деятельности ОВД может повысить эффективность, безопасность и прозрачность работы правоохранительных органов. Однако необходимо внимательно рассматривать применение этой технологии, учитывая все вызовы и особенности.

Важно понимать, что переход к использованию распределенных реестров требует тщательного планирования и адаптации существующих систем. Органы внутренних дел должны учесть потребности в обучении сотрудников, разработке соответствующих процедур и внедрении современных технологических решений для интеграции распределенных реестров в их деятельность.

СПИСОК ЛИТЕРАТУРЫ

1. Агиевич И. Перехват трафика как вектор атаки на пользователей блокчейн-проектов. [Электронный ресурс]. URL: habr.com›ru/companies/pt/articles/735756/ (дата обращения 14.07.2023).
2. Багин Д. Аспекты безопасности решений на основе распределенного реестра в свете российских требований. презентация выступления на конференции РусКрипто 2019. [Электронный ресурс]. URL: https://www.ruscrypto.ru/resource/archive/rc2019/files/12_Bagin.pdf?ysclid=lncyryyw6z730795414 (дата обращения 14.07.2023).
3. Нормативная база в области технологий распределенного реестра и блокчейн: промежуточный отчет о НИР / Рабочая группа № 2. ТК-159 рук. Панков К. М., 2019. 61 с.
4. Pankov K. N. Testing, verification and validation of distributed ledger systems // 2020 Systems of Signals Generating and Processing in the Field of on Board Communications. Moscow, Russia, 2020. С. 1-9.
5. What Is DLT (Distributed Ledger Technology)? [Электронный ресурс]. URL: https://101blockchains.com/what-is-dlt/ (дата обращения 14.07.2023).
6. What is distributed ledger technology? [Электронный ресурс]. URL: https://www.bis.org/publ/qtrpdf/r_qt1709y.htm (дата обращения 14.07.2023).
7. Secure and secret cooperation in robot swarms [Электронный ресурс]. URL: https://www.science.org/doi/10.1126/scirobotics.abf1538 (дата обращения 14.07.2023).

УДК 004.056

ОБОСНОВАНИЕ НЕОБХОДИМОСТИ СОВЕРШЕНСТВОВАНИЯ МЕТОДОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ВЕДОМСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Якушев Денис Игоревич, Жалдак Анастасия Алексеевна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: d.i.ya@yandex.ru, nastena161999@yandex.ru

Аннотация. В статье рассмотрены методы по совершенствованию практики организации защиты персональных данных, действующей в системе МВД России.

Ключевые слова: персональные данные; информационные системы; защита информации; угрозы безопасности информации; система технической защиты персональных данных.

JUSTIFICATION OF THE NEED TO IMPROVE THE METHODS OF PERSONAL DATA PROTECTION IN DEPARTMENTAL INFORMATION SYSTEMS

Yakushev Denis, Zhaldak Anastasia
St. Petersburg University of the Ministry of Internal Affairs of Russia
1 pilot Pilyutova st., St. Petersburg, 198206, Russia
e-mails: d.i.ya@yandex.ru, nastena161999@yandex.ru

Resume. The article discusses methods for improving the practice of organizing the protection of personal data operating in the system of the Ministry of Internal Affairs of Russia.

Keywords: personal data; information systems; information protection; information security threats; system of technical protection of personal data.

Современное российское общество характеризуется интенсивным развитием и стремительным внедрением информационных технологий во все сферы жизнедеятельности человека, преподнося информацию в качестве одного из основных ресурсов. В связи с этим, необходимо уделять особое внимание вопросу защиты информации и, в частности, защите персональных данных. Это связано прежде всего с гарантией конституционных прав и свобод граждан, а также активизацией различных хакерских группировок и спецслужб недружественных государств. Организация защиты персональных данных в информационных системах персональных данных в системе Министерства внутренних дел России (далее — МВД России) — одна из актуальных задач развития ведомства на современном этапе.

Совершенствования методов защиты персональных данных

В настоящее время уже существует сложная система нормативно-правового закрепления понятия персональных данных, основу которой составляют нормативные акты, распределенные по иерархии законодательства. Само понятие «персональных данных» определено как в международном, так и в отечественном отраслевом законодательстве, также оно присутствует в специализированных законах, регулирующих взаимоотношения в сфере сбора, обработки и защиты персональных данных в отдельных информационных системах, например, в органах внутренних дел.

В сфере международного правового регулирования защиты персональных данных сейчас можно выделить три равнозначных и непосредственно связанных тенденции:

1. Защита персональных данных является одной из неотъемлемых составляющих всеобщей системы, созданной для уважения и защиты прав человека. Законодательные нормы, которые регулируют данную сферу, разрабатываются в рамках всеобщих, гуманитарных принципов.

2. Органы управления Евросоюза, такие как Совет Европы и Еврокомиссия, а также руководящие органы, действующие в рамках евразийской экономической комиссии и других международных организаций, устанавливают технические и организационные стандарты, а также процессы обработки информации и защиты данных в рамках единого информационного пространства. Эти нормы обладают практическим значением и прямо регулируют превентивные и защитные меры, а также ответственность за нарушение права личности на защиту персональных данных.

3. Внутри договоров и конвенций, заключаемых между несколькими странами, также возникают соглашения, относящиеся к конфиденциальности информации о гражданах, передаче этих данных компетентным органам и процедурам обмена персональными данными между представителями стран-участников.

Что касается Российской федерации, то право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений декларировано Конституцией Российский Федерации. Для обеспечения защиты персональных данных в Российской Федерации были приняты два нормативно-правовых акта, непосредственно регулирующих данную сферу общественных отношений. К ним относятся Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [1].

Важная роль в системе нормативно-правового регулирования вопроса о защите персональных данных отведена Постановлению Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Данным постановлением установлено четыре уровня защищенности персональных данных при их обработке в информационных системах, а также требования для каждого из них. Постановлением также устанавливается требование использования средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

В информационных системах персональных данных МВД России существует целый ряд различных угроз персональным данным. Они подробно описаны в нормативные и научно-правовые источники, в которые включены как международные, так и отраслевые стандарты Российской Федерации по информационной

безопасности информационных систем. Также к данным источникам относятся нормативно-методическая документации ФСТЭК России, посвященная разработке базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных; ведомственная документации МВД России, регламентирующая требования по защите информации на объектах информатизации органов внутренних дел; научно-техническая литература в области обеспечения информационной безопасности [2].

Проанализировав нормативные и научно-правовые источники, можно сделать вывод, что круг угроз персональным данным достаточно обширен, и поэтому, можно предложить классифицировать основные угрозы в информационных системах персональных данных:

В первом случае, обратим внимание на аспект информационной безопасности, на которую направлена угроза. То есть, угрозы, направленные на нарушение целостности, доступности и конфиденциальности сведений, составляющих персональные данные. Основным требованием, предъявляемым к процессу сбора, обработки и хранения персональных данных выступает обеспечение конфиденциальности. Сведения о персональных данных не должны подвергаться утечкам, незаконному распространению.

Во втором случае, обратимся к природе угрозы, то есть к источнику угрозы. Здесь выделяются как преднамеренные, так и непреднамеренные угрозы. В качестве преднамеренных выделяют отказы и сбои аппаратного обеспечения компьютерных систем, ошибки в программном обеспечении, ошибки в работе пользователей информационных систем и персонала по их обслуживанию, помехи в линиях связи из-за воздействий внешней среды, аварийные ситуации из-за стихийных бедствий и различного рода техногенных аварий. К непреднамеренным угрозам относятся целенаправленные действий конкретных лиц, направленные на негативные воздействия по отношению к сведениям, содержащим персональные данные, в информационных системах персональных данных МВД России.

Несмотря на многообразие возможных угроз по отношению к персональным данным, обрабатываемым в информационных системах персональных данных в МВД России, их реализация приводит к крайне негативным и опасным последствиям. Последствия могут быть направлены как на непосредственного сотрудника (работника), так и в отношении к системе органов внутренних дел в целом.

Наличие угроз персональным данным в информационных системах обуславливает необходимость в организации системы защиты в данной области информационной безопасности. Сейчас данная система защиты строится на определении и последовательной реализации организационных способах, каждый из которых представлен в виде совокупности однородных действий, процессов и операций, направленных на достижение защиты персональных данных.

Прежде всего, это нормативно-правовой способ, заключающийся в издании нормативных правовых актов, в рамках которых закрепляются конкретные требования, стандарты и порядок сбора, обработки, хранения и использования персональных данных в информационных системах персональных данных МВД России.

Вторым способом выделим — организационный, который заключается в регламентации доступа к информационным и вычислительным ресурсам, функциональным процессам систем обработки данных, к регламентации деятельности сотрудников.

Третьим способом назовем — программно-аппаратный, заключающийся в использовании специализированных программ, соответствующего программного оборудования и иных устройств, которые позволяют минимизировать риски утечки персональных данных из информационных систем персональных данных МВД России.

Четвертый способ — технический, который направлен непосредственно на организацию физической защиты и использование технических средств, предотвращающих или существенно затрудняющих утечку информации.

Пятый способ — технологический, то есть выполнение определенных процедур, для сохранения данных (например, создание архивных копий массивов информации, регистрация пользователей в журналах).

Шестой способ — криптографический, предназначенный для осуществления криптографического преобразования информации.

И седьмой способ — личностный, оттого насколько четко пользователи будут понимать, как правильно работать с данными в информационных системах, зависит результат сохранения персональных данных.

Вышесказанное позволяет отметить значимость разработки новых конкретных методов по совершенствованию практики организации защиты персональных данных в ведомственных информационных системах.

СПИСОК ЛИТЕРАТУРЫ

1. Минзов А. С. Безопасность персональных данных: новый взгляд на старую проблему // Вопросы кибербезопасности. 2022. № 4(50). С. 2-12.
2. Соболев А. А. Защита персональных данных в организации, обработанных в электронном виде // Трибуна ученого. 2022. № 11. С. 134-142.
3. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и органах местного самоуправления: учебно-методическое пособие / В. А. Мещеряков [и др.] ; под ред. В. А. Мещерякова. Воронеж : Правительство Воронежской области, 2016. 208 с.

УДК 004.056

ГРУППОВАЯ ПОЛИТИКА БЕЗОПАСНОСТИ КАК СПОСОБ ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Якушев Денис Игоревич, Лукина Ксения Сергеевна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: d.i.ya@yandex.ru, kseni.luk@yandex.ru

Аннотация. Рассмотрены особенности групповой политики безопасности, направленной на повышения защищённости объектов информатизации органов внутренних дел.

Ключевые слова: кибербезопасность; информационная безопасность; групповая политика безопасности; объекты информатизации; объекты групповой политики.

GROUP SECURITY POLICY AS A WAY TO INCREASE THE SECURITY OF OBJECTS OF INFORMATIZATION OF INTERNAL AFFAIRS BODIES

Yakushev Denis, Lukina Ksenia
St. Petersburg University of the Ministry of Internal Affairs of Russia
1 Letchik Pilyutov St, St. Petersburg, 198206, Russia
e-mail: d.i.ya@yandex.ru, kseni.luk@yandex.ru

Abstract. The features of the group security policy aimed at increasing the security of objects of informatization of internal affairs bodies are considered.

Keywords: cybersecurity; information security; group security policy; informatization objects; group policy object.

Защита информации в отдельном компьютере уже требует некоторых знаний и навыков в области информационной безопасности. Если же множество компьютеров объединены в локальную сеть с выходом в Интернет, то задача обеспечения информационной безопасности значительно усложняется и не имеет однозначного решения. Одним из способов решения этой задачи является выработка групповой политики безопасности, обеспечивающей приемлемый уровень защищенности. Поэтому для объектов информатизации органов внутренних дел рассматриваемый вопрос является актуальным.

Групповая политика безопасности как способ повышения защищённости объектов информатизации

Защита информации — это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Известно, что в основе деятельности по защите информации лежат регламентирующие нормативные правовые акты. Однако реализуются они только в том случае, если подкрепляются организаторской деятельностью соответствующих структур, создаваемых в государстве, ведомствах, учреждениях и организациях.

На организационном уровне должны решаться следующие задачи обеспечения безопасности информации:

- –ограничение доступа на объект и к ресурсам информации;
- –разграничение доступа к ресурсам информации;
- –разработка нормативных правовых документов по защите информации;
- –аттестация объектов информатизации;
- –совершенствование системы защиты информации;
- –оценка эффективности системы защиты информации;
- –контроль выполнения установленных правил работы в компьютерных системах.

Объект информатизации (в соответствии с ГОСТ Р 51275-2006, который распространяется на объекты информатизации, создаваемые и эксплуатируемые в различных областях деятельности, в том числе обороны, экономики, науки и других областях) — совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Одним из примеров объекта информатизации и информационного обеспечения органов внутренних дел является единая информационно-телекоммуникационная система (ЕИТКС) — основа информационно-аналитического обеспечения деятельности МВД России.

Единая информационно-телекоммуникационная система органов внутренних дел (ЕИТКС ОВД) — информационно-телекоммуникационная система, основанная на интегрированной транспортной среде органов внутренних дел, обеспечивающей взаимодействие с телекоммуникационной системой внутренних войск МВД России, телекоммуникационными системами органов государственной власти, включая правоохранительные органы, а также доступ сотрудников внутренних дел к услугам публичных и специальных федеральных информационно-телекоммуникационных систем и состоящая из автоматизированных банков данных общего

пользования на базе унифицированных программно-технических комплексов информационно-аналитических и экспертно-криминалистических центров органов внутренних дел.

Одной из основных целей разработки групповой политики безопасности в органах внутренних дел является предотвращение причинения ущерба деятельности объектов информатизации органов внутренних дел, который может быть причинен в результате нарушения целостности, доступности и конфиденциальности информации, хранимой в органах внутренних дел.

Групповая политика безопасности — это параметры, управляющие функционированием системы. Групповая политика упрощает администрирование, предоставляя администраторам централизованный контроль над привилегиями, правами и возможностями пользователей и компьютеров.

Групповая политика безопасности — важный инструмент для управления настройками безопасности, выполняющая задачи разграничения доступа пользователей, управления настройками безопасности базовой системы, включающую формирование политики пароля и блокировки учетной записи; обозначения ограничений для приложений и устройств, осуществления процедуры назначения прав пользователя при определении пользователей, имеющих право доступа к определенному набору серверов и рабочих станций через удаленный рабочий стол; использование политики групп с ограниченным доступом; управление службами операционной системы; управление политикой реестра и файловой системы; настройка политики ограниченного применения программ.

Объект групповой политики — это общее название набора файлов, директорий и записей, которые хранят настройки пользователя и определяют, какие параметры пользователь (администратор) может изменить с помощью групповой политики. Создание политики означает внесение изменений в объект групповой политики.

Для настройки параметров в операционной системе MS Windows 10 используется оснастка «Редактор локальной групповой политики». Данная оснастка служит для просмотра и редактирования объектов групповой политики (Group Policy Object, GPO), в которых хранятся параметры локальных политик для компьютера и пользователей. Оснастка «Редактор локальной групповой политики» позволяет изменять политику, распространяющуюся как на компьютеры, так и на пользователей.

В Microsoft Security Baseline содержатся рекомендованные настройки, которые Microsoft предлагает использовать на рабочих станциях и серверах Windows для обеспечения безопасной конфигурации для защиты контролеров домена, рядовых серверов, компьютеров и пользователей. На основе Microsoft Security Baseline разработаны эталонные групповые политики, которые администраторы могут использовать в своих доменах Active Directory. Настройки безопасности в групповой политике Microsoft Security Baseline позволяют администраторам обеспечить уровень защиты корпоративной инфраструктуры Windows, соответствующий актуальным мировым стандартам. Эталонная политика Microsoft Security Baseline входит в состав продукта Microsoft Security Compliance Manager (SCM). SCM это бесплатный продукт, в который входит несколько инструментов для анализа, тестирование и применения лучших и актуальных рекомендаций безопасности для Windows и других продуктов Microsoft.

Существуют шаблоны GPO Security Baseline для различных элементов инфраструктуры Windows: политики для компьютеров, пользователей, доменных серверов, контроллеров домена настройки Internet Explorer, BitLocker, Credential Guard, Windows Defender Antivirus. В папке GPOs хранятся готовая политика безопасности для различных сценариев использования Windows

В связи с переходом на отечественное программное обеспечение, регламентированное Указом Президента Российской Федерации от 30.03.2022 № 166, необходимо выделить несколько вспомогательных программ, необходимых для работы с групповой политикой безопасности на ОС Linux.

Для управления конфигурациями серверов, их обслуживания на всём жизненном цикле имеет актуальное значение связка работы трёх компонентов: foreman, puppet, ansible.

Foreman — инструмент, предназначенный для помощи системным администраторам в управлении серверами, обеспечивающий простой способ взаимодействия с системами управления конфигурациями (Ansible, Puppet и др.) для автоматизации задач администрирования и развертывания приложений. Foreman поддерживает web-интерфейс, API и CLI, которые можно использовать для предоставления, настройки и мониторинга серверов. Подходит для инфраструктур любых размеров.

Puppet — кроссплатформенное клиент-серверное приложение, которое позволяет централизованно управлять конфигурацией операционных систем и программ, установленных на нескольких компьютерах, позволяющий системным администраторам автоматизировать предоставление, настройку и управление серверной инфраструктурой. Требует установки агентского программного обеспечения на управляемые компьютеры. Puppet используется для приведения хостов к необходимому для обеспечения безопасности состоянию и поддержания этого состояния.

Ansible — система управления конфигурациями, использующаяся для автоматизации настройки и развертывания программного обеспечения. Позволяет автоматизировать сложные задачи, например, непрерывное развертывание или непрерывное обновление без простоев. Не требует установки агентского ПО на управляемые компьютеры. Работает с Linux-узлами (SSH-соединение), также поддерживает Windows (WinRM соединение).

Существуют программные комплексы, предназначенные для централизованного администрирования ресурсов домена в компьютерных сетях под управлением «Операционной системы специального назначения

«Astra Linux Special Edition» посредством графического интерфейса. Примером такого программного комплекса является ПК «ALD Pro», областью применения которого является автоматизация деятельности системных администраторов в рамках эксплуатации ИТ-инфраструктуры на базе ОС Astra Linux.

Групповая политика в реализации Active Directory — это часть интегрированного решения. Альтернативной реализацией Active Directory под Linux/Unix является проект Samba. Начиная с четвёртой версии, Samba может выступать в роли контроллера домена и сервиса Active Directory, совместимого с реализацией Windows 2000, и способна обслуживать все поддерживаемые Microsoft версии Windows-клиентов, в том числе Windows 10. Samba работает на большинстве Unix-подобных систем, таких как Linux. Samba включена практически во все дистрибутивы Linux.

В статье были рассмотрены некоторые средства разработки групповой политики безопасности, позволяющие обеспечить приемлемый уровень информационной защищенности объектов информатизации органов внутренних дел.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию : офиц. издание. М. : Стандартинформ, 2007.
2. Групповые политики (GPO) Active Directory: разбираемся почему это важно и как ими управлять в GPOAdmin // habr.com [Электронный ресурс]. URL: https://habr.com/ru/companies/galssoftware/articles/543588/ (дата обращения: 20.08.2023).
3. Козьминых С. И. Организация защиты информации в органах внутренних дел : учеб. пособие. Ч. I. М. : Московский университет МВД России, 2013. 167 с.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

УДК 004.451:004.056

ПРОБЛЕМА БЕЗОПАСНОСТИ ПРИ СБОРЕ, ХРАНЕНИИ И ИСПОЛЬЗОВАНИИ ДАННЫХ ПРИ РАБОТЕ С ЦИФРОВЫМИ ДВОЙНИКАМИ ЛЮДЕЙ

Ананьева Варвара Яновна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
e-mail: viaananeva@etu.ru

Аннотация. В данной работе рассматриваются вопросы безопасности сбора, хранения и использования данных, которые используются для работы цифровых двойников людей.

Ключевые слова: цифровой двойник; цифровой двойник человека; безопасность данных; защита данных; здравоохранение; медицина.

THE PROBLEM OF SECURITY IN GATHERING, STORING AND USING DATA WHEN WORKING WITH DIGITAL TWINS OF PEOPLE

Ananeva Varvara
Saint-Petersburg Electrotechnical University
5 Professor Popov St, St. Petersburg, 197022, Russia
e-mail: viaananeva@etu.ru

Abstract. Publication issues of security of gathering, storing and using data, which is used for the work of digital twins of people, are considered.

Keywords: digital twin; digital twinof human; data security; data protection; healthcare; medicine.

Цифровой двойник (DigitalTwin, ЦД) [1] — сложное понятие, коротко которое можно определить, как виртуальную сущность, которая состоит из виртуальной модели и процессора, который обрабатывает запросы к модели и отвечает за её адекватность. ЦД можно применять в различных областях [2], в том числе в здравоохранении. Применение ЦД в здравоохранении очень важный шаг в развитии медицины, использование ЦД может принести много пользы, как врачам, так и пациентам. Примеры ЦД и их применение в медицине:

– ЦД человека — тела человека, его органов;
– ЦД в дистанционной хирургии;
– ЦД медицинского учреждения (больницы, поликлиники) — для административного управления медицинской организацией.

ЦД сопровождает объект на протяжении всего его жизненного цикла. В здравоохранении ЦД можно использовать, как полную цифровую копию человека, которая поддерживается в актуальном состоянии и на основе которой можно предсказывать будущее состояние, тестировать и выбирать наиболее подходящий вариант лечения и т.д. Например, уже сейчас создают ЦД органов человека [3, 4]. Одна из возможностей ЦД — это предсказание на основе текущих данных и, собранных ранее, исторических. Эти данные необходимы, чтобы с помощью алгоритмов машинного обучения создать модель, которая в дальнейшем с высокой степенью вероятности будет выдавать результат. Одной из проблем является сбор и хранение этих данных. Можно обезличивать информацию, но человек, данные которого были собраны, всё равно может быть не до конца уверен, что обезличивание произошло. Это происходит из-за «сливов» персональных данных, полученных из банков, системы «Госуслуги», от телефонных операторов, системы ГИБДД и др. Таким образом, человеку сложно переступить барьер и даже в благородных целях — помочь себе и другим людям, — отдать свои биометрические данные, данные о состоянии здоровья и т.д.

Таким образом, при создании ЦД людей необходимо:

– продумать вопрос о безопасной передаче и хранении данных человека, о том, какой медицинский работник, какую информацию может видеть, как и где он её обрабатывает, есть ли у него возможность сохранить данную информацию;
– осветить пользователям системы все возможные небезопасные моменты использования данных, рассказать людям, что данные защищены, каким образом это происходит. Если у пациентов будет доступ к такой информации, доверие к ЦД будет только расти.

Таким образом, пока цифровые двойники людей ещё на стадии развития и повсеместно не внедрены, необходимо готовить людей к их использованию путём освещения их возможностей, рассказывая, как они устроены и работают, чтобы люди, данные которых будут использоваться, не считали, что их можно украсть, обнародовать, использовать в качестве контролирующего, шантажирующего воздействия. Также «продвигать» ЦД и пытаться понять страхи и переживания людей можно путём опросов об отношении к ЦД, о наличии, доступности, качестве предлагаемой информации.

СПИСОК ЛИТЕРАТУРЫ

1. Grieves Grieves M. Originsofthe Digital Twin Concept. Florida Institute of Technology // NASA. 2016. DOI:10.13140/RG.2.2.26367.61609.
2. Vohra M. Digital Twin Technology. Fundamentals and Applications.USA: Scrivener Publishing and Wiley, 2023.
3. Цифровой двойник сердца // ZDRAV.EXPERT : Медтех-портал. [Электронный ресурс]. URL: https://zdrav.expert/index.php // Продукт:Цифровой_двойник_сердца (дата обращения 14.06.2023).
4. ЛЭТИ: Цифровой двойник шеи // ZDRAV.EXPERT: Медтех-портал. [Электронный ресурс]. URL: https://zdrav.expert/index.php/ Продукт:ЛЭТИ_Цифровой_двойник_шеи (дата обращения 14.06.2023).

УДК 004.082.2

МОДЕЛЬ ВЫРАБОТКИ РЕСУРСА ТВЕРДОТЕЛЬНЫХ НАКОПИТЕЛЕЙ

Архипцев Евгений Дмитриевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5 лит. Ф, Санкт-Петербург, 19702, Россия
e-mail: lokargenia@gmail.com

Аннотация. Рассматривается задача оценивания параметра выработки ресурса до критического состояния из-за износа твердотельных накопителей. Приводятся математические выражения показателей, позволяющих оценить полный ресурс системы хранения данных во времени, что позволяет планировать выделение ресурса в условиях больших данных.

Ключевые слова: большие данные, система хранения данных, твердотельный накопитель, ресурс накопителя, показатели выработки ресурса накопителя.

MODEL OF LIFE DEVELOPMENT OF SOLID-STATE DRIVES

Arkhiptsev Evgeny
Saint Petersburg Electrotechnical University «LETI»
5 Professor Popov St, lit. F, St. Petersburg, 197376, Russia
e-mail: lokargenia@gmail.com

Abstract. The problem of estimating the resource depletion parameter to a critical state due to the wear of solid-state drives is considered. Mathematical expressions of indicators are given that allow estimating the full resource of the data storage system in time, which makes it possible to plan the allocation of a resource in the conditions of big data.

Keywords: big data, storage system, solid state drive, drive life, drive life metrics.

Одной из важнейших характеристик и особенностей всех твердотельных накопителей является их ресурс. Данная характеристика зависит от конструктивного параметра твердотельных накопителей — общего ресурса записи Q_{DISK}, выражаемого в количестве байт. Также для оценки среднего времени жизни твердотельного накопителя, совместно с общим ресурсом записи, используется средняя интенсивность потока записи/перезаписи данных [1].

По наблюдению ряда исследователей, износ твердотельных накопителей в следствие операций перезаписи ведёт к усиленному потоку отказов системы хранения данных в ходе постепенной выработки ресурса твердотельного накопителя. С целью введения данной особенности в математическую модель необходимо выразить интенсивность отказов твердотельных накопителей через две компоненты [2, 3]:

– интенсивность внезапных (случайных) отказов твердотельных устройств хранения;

– интенсивность отказов твердотельного накопителя, возникающих в соответствие с постепенным износом, выработкой ресурса.

Наличие данных компонент основано на природе возникающих отказов. Любой твердотельный накопитель может выйти из строя как при появлении функционального (внезапного) отказа, так и в случае постепенного отказа, связанного с выработкой ресурса. Общая (суммарная) вероятность отказа твердотельного накопителя равна вероятности наступления либо функционального отказа, либо отказа за счёт износа, за вычетом вероятности наступление обоих данных событий [4].

Введены следующие допущение в модель выработки ресурса:

1. Случайный и постепенный отказы являются независимыми и совместными событиями.
2. Отказы устройств хранения распределены по экспоненциальному закону.
3. Данные равномерно записываются на все устройства хранения системы.

Выделены следующие виды отказов:

– Функциональный отказ — выражается при помощи параметра среднего времени наработки на отказ.
– Скрытая ошибка.

Ресурс каждого накопителя в системе хранения обозначен через конструктивный параметр Q_{DISK}, задаваемого производителем устройства при изготовлении. Ресурс вырабатывается в следствие записи/перезаписи данных на твердотельных накопителях. При этом полезные данные записываются в систему хранения только на блоки, относящиеся к информационной (полезной) ёмкости.

Выведены выражения:

– информационной ёмкости системы хранения данных, использующая схему кодирования (k+r), где k — количество информационных узлов, r — число избыточных узлов;
– ресурса записи системы хранения данных, построенной на основе твердотельных накопителей;
– коэффициента запаса устойчивости ресурса циклов перезаписи.
– полный ресурс системы хранения данных.

Выражения позволяют оценить приблизительный параметр выработки ресурса до критического состояния из-за износа твердотельных накопителей:

Приведённые показатели позволяют оценить полный ресурс системы хранения данных во времени, с целью оценки выходных параметров модели надёжности системы хранения данных.

СПИСОК ЛИТЕРАТУРЫ

1. Пойманова Е. Д., Татарникова Т. М., Краева Е. В. Модель управления хранением трафика данных // Известия высших учебных заведений. Приборостроение. 2021. Т. 64. № 5. С. 370-375.
2. Советов Б. Я., Татарникова Т. М., Пойманова Е. Д. Модель управления масштабированием хранилища // Информационные и управляющие системы. 2020. № 5(108). С. 43-49. DOI: 10.31799/1684-8853-2020-5-43-49.
3. Татарникова Т. М., Архипцев Е. Д. Определение числа реплик распределенного хранения больших данных // Международная конференция по мягким вычислениям и измерениям. 2023. Т. 1. С. 305-308.
4. Татарникова Т. М., Пойманова Е. Д. Энергетическая модель процесса хранения данных // Информация и космос. 2019. № 1. С. 89-95.

УДК 004.056

ОГРАНИЧЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СРЕДСТВ ИСПРАВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ВО ВРЕМЯ ЕГО ВЫПОЛНЕНИЯ

Валеев Денис Рашидович, Котенко Игорь Витальевич
СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: lemniscattaden@gmail.com, ivkote@comsec.spb.ru

Аннотация. В настоящее время существует множество средств исправления программного обеспечения (для удаления уязвимостей) в режиме реального времени, в то же время многие широко используемые программные системы их не реализуют, вынуждая пользователей эксплуатировать неисправленное программное обеспечение либо прерывать работу системы для её обновления. В работе проанализированы доступные на сегодняшний день программные решения для исправлений в режиме реального времени, их ограничения и возможные направления их улучшения.

Ключевые слова: информационная безопасность; обновление программного обеспечения; исправление уязвимостей.

LIMITATIONS AND OUTLOOK FOR SOFTWARE RUNTIME PATCHING TOOLS

Valeev Denis, Kotenko Igor
SPIIRAS – SPCRAS
39 14th line, V. I., St. Petersburg, 199178, Russia
e-mail: lemniscattaden@gmail.com, ivkote@comsec.spb.ru

Abstract. At present, there are many approaches to apply software patches in real time, at the same time many widely used software systems do not implement them, forcing users to operate unpatched software or interrupt the system to update it. The paper analyzes the currently available software solutions for applying patches in real time, their limitations and possible directions for their improvement.

Keywords: information security, software update, vulnerability fix.

Задача анализа уязвимостей и своевременного применения исправлений (патчей) к программному обеспечению является актуальной в настоящее время [1-3]. При решении данной задачи зачастую изменения не применяются вовремя потому, что их применение требует прерывания работы системы, что снижает показатель времени безотказной работы и доставляет неудобство пользователям [4]. Промедление в применении изменений зачастую имеет драматические последствия [5], когда вопрос касается безопасности использования неисправленной версии программного обеспечения.

Для решения этой задачи индустрия предлагает программные решения, осуществляющие применение исправлений без прерывания работы системы или с незначительным временем простоя. На текущий момент предложено множество вариантов реализации механизмов обновления программного обеспечения в режиме реального времени [6]. Несмотря на это значительная часть современных программных систем до сих пор требует длительной остановки работы для применения обновлений. Некоторые поставщики программного обеспечения

пошли по пути принуждения к обновлению с перезапуском вместо реализации обновлений в режиме реального времени, чем многие пользователи остались недовольны [7].

Понимание недостатков подходов для применения исправлений в режиме реального времени, их исправление и широкое внедрение существенно повысят безопасность и удобство эксплуатации сложных программных систем, таких как серверы, мобильные устройства и т.п.

В работе проанализированы доступные на сегодняшний день программные решения для применения исправлений в режиме реального времени, их ограничения и возможные направления их улучшения.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Kotenko I., Stepashkin M. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science. 2005. Vol. 3685. Pp. 311-324.
2. Котенко И. В., Степашкин М. В., Богданов В. С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006, №. 2, С.7-24.
3. Котенко И. В., Десницкий В. А., Чечулин А. А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд, 2011. № 3. С. 68-75.
4. Rajivan P., Aharonov-Majar E., Gonzalez C. Update now or later? Effects of experience, cost, and risk preference on update decisions // Journal of Cybersecurity, Vol. 6, Issue 1. 2020. Pp. 1-20. doi: 10.1093/cybsec/tyaa002.
5. What is WannaCry ransomware? // Kaspersky. URL: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry (дата обращения: 06.07.2023).
6. Chadni I., Prokhorenko V., Babar M. A. Runtime Software Patching: Taxonomy, Survey and Future Directions // Journal of Systems and Software. Vol. 200, June 2023, 111652. Pp. 1-22. https://doi.org/10.1016/j.jss.2023.111652.
7. Morris J., Becker I., Parkin S. In Control with no Control: Perceptions and Reality of Windows 10 Home Edition Update Features // Workshop on Usable Security (USEC) 2019. 24 February 2019, San Diego, CA, USA. Pp. 1-18. http://dx.doi.org/10.14722/usec.2019.23008.

УДК 004.056

РАЗРАБОТКА СТЕНДА ДЛЯ ДИНАМИЧЕСКОГО АНАЛИЗА ЭКСПЛОЙТОВ

Веревкин Сергей Александрович, Федорченко Елена Владимировна
СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: vrjovkin@rambler.ru, doynikova@comsec.spb.ru

Аннотация. В работе предложено решение задачи разработки стенда для проведения динамического анализа вредоносного кода. Основной целью анализа исходного кода эксплойтов является получение объективных показателей реализации атакующих воздействий и использования этих данных в системе оценивания защищенности.

Ключевые слова: информационная безопасность, оценка защищенности, эксплойт, уязвимость, динамический анализ эксплойтов.

DEVELOPMENT OF THE TESTBED FOR DYNAMIC ANALYSIS OF EXPLOITS

Verevkin Sergey, Fedorchenko Elena
SPIIRAS – SPCRAS
39 14th Line, V. I., St. Petersburg, 199178, Russia
e-mails: vrjovkin@rambler.ru, doynikova@comsec.spb.ru

Abstract. The paper proposes a solution to the problem of developing the testbed for dynamic analysis of malicious code. The main purpose of analyzing the source code of exploits is to obtain objective indicators of the implementation of attacking impacts and the use of these data in the security assessment system.

Keywords: information security, security assessment, exploit, vulnerability, dynamic malware analysis.

На сегодняшний день существует актуальная проблема, связанная с оцениванием рисков информационной безопасности. Среди основных причин данной проблемы следует выделить сложность устройств в сети, количество которых постоянно меняется, появление новых, ранее неизвестных кибератак, а также отсутствие объективной оценки последствий кибератак. В данной работе рассматривается задача разработки стенда для динамического анализа эксплойтов, а именно, для выявления признаков их выполнения и, в конечном итоге, получения объективных оценок защищенности.

В рамках исследования проведено сравнение современных методов динамического анализа эксплойтов [1] и подходов к формированию среды для проведения испытаний [2]. В результате, определены требования к среде проведения испытаний, выбраны средства моделирования, а также составлен перечень уязвимостей и эксплойтов, тестирование которых будет проводиться для получения исходных данных.

Чтобы обеспечить полноту и масштабируемость решения, было решено использовать средства виртуализации. Также, стоит отметить еще одно преимущество использования технологии виртуализации. Оно заключается в возможности оперативного восстановления работоспособности виртуальных устройств в случае их повреждения при запуске вредоносного кода.

В качестве среды моделирования сетевой инфраструктуры и телекоммуникационного оборудования выбрано решение EVE-NG, обеспечивающее возможность гибкой настройки конечных узлов, а также широкий

выбор моделируемого сетевого оборудования. Конечными узлами (хостами) является набор уязвимых виртуальных машин Metasploitable версий 1/2/3, а также виртуальные машины из облачного хранилища средства создания и конфигурирования виртуальных машин Vagrant.

Выбранные виртуальные машины изначально имеют уязвимую конфигурацию, что делает возможным проведение тестирования уязвимостей конкретного программного и программно-аппаратного обеспечения. Однако, в связи с ежедневной актуализацией баз существующих уязвимостей, проведено повторное сканирование уязвимостей каждой виртуальной машины в составе стенда с помощью сканера уязвимостей OpenVAS. На основе результатов сканирования сформирован перечень актуальных уязвимостей, имеющих эксплойт. Поиск эксплойтов выполнен на основе открытых баз данных, таких как ExploitDB.

В результате проделанной работы развернут виртуальный макет сети, содержащий перечень необходимых уязвимостей. Также определен план проведения эксперимента для получения исходных данных, а именно — системных журналов и сетевого трафика. В качестве планируемых результатов работы предполагается разработка автоматизированной системы комплексного оценивания рисков информационной безопасности.

Работа выполнена при поддержке гранта РНФ № 23-21-00498 в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Cafasso M., Tarral M. Designing flexible sandboxing solutions to adapt to new malware trends // Computer Fraud & Security, 2018. № 2. Pp. 5-9. ISSN 1361-3723. [Электронный ресурс]. URL: http://www.sciencedirect.com/science/article/pii/S1361372318300137 (дата обращения: 08.06.2023).
2. Bird K. Sandboxing: a line in the sand against malware // Network Security. 2014, № 4. Pp. 18-20. ISSN 1353-4858. [Электронный ресурс]. URL: https://www.researchgate.net/publication/261839360_Sandboxing_A_line_in_the_sand_against_malware (дата обращения: 08.06.2023).
3. Среда виртуализации и эмуляции сетевого взаимодействия EVE-NG [Электронный ресурс]. URL: https://eve-ng.ru/ (дата обращения: 08.06.2023).
4. Средство для управление виртуальными машинами Vagrant [Электронный ресурс]. URL: https://www.vagrantup.com/ (дата обращения: 08.06.2023).

УДК 004.056

ПОСТРОЕНИЕ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ ФЕДЕРАТИВНОГО ОБУЧЕНИЯ

Голубев Сергей Александрович, Новикова Евгения Сергеевна
СПИИРАН – СПб ФИЦ РАН
14 линия, 39, Санкт-Петербург, 199178, Россия
e-mail: ser9800@mail.ru, novikova@comsec.spb.ru

Аннотация. Применение федеративного обучения позволяет строить распределенные системы обнаружения вторжений, которые не требуют передачи данных, генерируемых на местах, для обучения и дообучения моделей, используемых для выявления атак и аномалий в информационных системах. В настоящем докладе представляется архитектура распределенной системы обнаружения вторжений, обсуждаются требования к вычислительным ресурсам компонентов, выполняющих локальное обучения моделей. Предлагается подход к моделированию распределения данных между несколькими объектами, являющимися владельцами данных, обсуждаются настройки федеративного обучения и их влияние на процесс формирования глобальной модели обнаружения вторжений.

Ключевые слова: обнаружение вторжений, распределенные системы, федеративное обучение, машинное обучение.

DESIGN OF A DISTRIBUTED INTRUSION DETECTION SYSTEM BASED ON FEDERATED LEARNING

Golubev Sergei, Novikova Evgenia
SPIIRAS – SPCRAS
39 14th Line St, Petersburg, 199178, Russia
e-mail: ser9800@mail.ru, novikova@comsec.spb.ru

Abstract. The application of federated learning allows constructing distributed intrusion detection systems that do not require the transfer of locally generated data to train and retrain models used to detect attacks and anomalies in information systems. This paper presents the architecture of a distributed intrusion detection system, discussing the computational resource requirements of the components that perform local model training. An approach for modeling the distribution of data among multiple data-owning objects is proposed, and the federated learning settings and their impact on the global intrusion detection model generation process are discussed.

Keywords: intrusion detection, distributed systems, federated learning, machine learning.

Концепция федеративного обучения как способ построения распределенных информационных систем, в которых аналитические модели формируются совместно несколькими участниками была предложена в 2016 году [1]. Ее отличительной особенностью является возможность формировать глобальные аналитические модели на множестве наборов данных, которые генерируются различными объектами и /или субъектами, без их непосредственной передачи в единое хранилище данных. Благодаря этому решаются проблемы, связанные с использованием данных с ограниченным доступом. Естественным образом расширяется обучающая выборка,

которая используется при обучении аналитических моделей, что позволяет расширять набор детектируемых типов атак и аномалий.

В настоящем докладе представляется архитектура распределенной системы обнаружения вторжений, в которой формирование моделей обнаружения вторжений осуществляют с помощью федеративного обучения, а также представляется ее программный прототип. Особое внимание в докладе уделено проблеме моделирования распределения данных между несколькими участниками или объектами-владельцами данных. Рассмотрены две схемы моделирования взаимодействия данных с использованием одного и нескольких наборов данных [2, 3]. В первом случае один набор данных распределяется между несколькими клиентами, а во втором случае каждый клиент владеет разными наборами данных, однако в этом случае необходимо привести множество атрибутов в разных наборах данных к единому подмножетсву.

Применение федеративного обучения накладывает ряд дополнительных требований к вычислительным ресурсам компонентов, осуществляющих обучение моделей в федеративном режиме. Для оценки данных требований и их влияния на производительность компонентов СОВ была разработана методика оценивания эффективности обнаружения вторжений, которая включает не только метрики, характеризующие точность выявленных атак и долю ложноположительных срабатываний, а также время обучения моделей, загрузку ЦПУ, объем передаваемого трафика. В докладе обсуждается влияние различных настроек федеративного обучения на значения данных параметров.

Исследование выполнено за счет гранта Российского научного фонда (проект № 22-21-00724).

СПИСОК ЛИТЕРАТУРЫ

1. McMahan H. B. Communication-Efficient Learning of Deep Networks from Decentralized Data / McMahan H. B. [и др.] // AISTATS. 2017.
2. Zhao R.. Semi-Supervised Federated Learning Based Intrusion Detection Method for Internet of Things / Zhao R. [и др.] // IEEE Internet of Things Journal. 2022. С. 1. DOI: 10.1109/JIOT.2022.3175918.
3. Popoola S. I. Federated Deep Learning for Collaborative Intrusion Detection in Heterogeneous Networks / Popoola S. I. [и др.] // 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall). 2021. С. 1-6. DOI: 10.1109/VTC2021-Fall52928.2021.9625505.

УДК 004.056.5

ОБЗОР И СИСТЕМАТИЗАЦИЯ АКТУАЛЬНЫХ МЕТОДОВ РЕАЛИЗАЦИИ ФИШИНГОВЫХ АТАК

Горда Максим Дмитриевич, Чечулин Андрей Алексеевич
СПИИРАН – СПб ФИЦ РАН
14-я линия В. О, 39, лит. А, Санкт-Петербург, 199178, Россия
e-mails: m.gorda.lengu@ya.ru, andreych@bk.ru

Аннотация: Фишинговые атаки являются актуальным средством совершения мошеннических действий в Интернете. Если раньше такие атаки имели примитивный характер, в силу отсутствия различных систем защиты, а также неосведомленности пользователей сети Интернет, то на данный момент злоумышленниками изобретаются более сложные методы реализации фишинга. В данной статье рассматриваются актуальные методы реализации фишинговых атак злоумышленниками.

Ключевые слова: информационная безопасность, кибератаки, анализ кибератак, фишинговые атаки, техники фишинговых атак, методы реализации фишинга.

REVIEW AND SYSTEMATIZATION OF RELEVANT PHISHING ATTACKS TECHNIQUES

Gorda Maxim, Chechulin Andrey
SPIIRAS – SPCRAS
39 14th Line of Vasilevskiy Island, lit. A, St. Petersburg, 199178, Russia
e-mails: m.gorda.lengu@ya.ru, andreych@bk.ru

Abstract: Phishing attack is an actual mean of fraudulent actions committing on the Internet. Formerly such attacks were primitive, due to the lack of protection systems, as well as the ignorance of Internet users. Now malefactors are inventing more and more complex methods of phishing implementation. The paper discusses relevant methods of phishing attacks.

Keywords: information security, cyberattacks, cyberattack analysis, phishing attacks, phishing attack techniques, phishing implementation methods.

Со значительным ростом популярности сети Интернет, а также реализации политик цифровизации как в отдельных организациях, так и в стране в целом увеличилась и активность преступников и преступных групп в цифровом поле. В результате действий злоумышленников огромное количество финансовой, конфиденциальной, личной и даже секретной информации находится под угрозой. Каким бы не был уровень автоматизации или цифровизации в организациях, в любом случае влияние и присутствие человека на уровне управления и контроля остаётся неизменным. Для защиты необходимых данных в организациях создают системы защиты информации, которые нацелены на повышение защищённости пользователей информационных систем.

Злоумышленники пытаются каждый день организовать атаки на системы защиты организаций, однако не всегда могут реализовать свои преступные действия. Для того, чтобы преодолеть защиту потенциальный преступник может воспользоваться методами социальной инженерии, которые, в некоторых случаях, будут более

эффективны. Также такие методы не требуют технических навыков от хакеров, иногда достаточно иметь определённые данные о потенциальной жертве и уметь правильно манипулировать ими.

Одним из видов социальной инженерии [1] являются фишинговые атаки, которые наравне с техническими атаками являются серьезной угрозой для защищаемых данных и объектов.

Актуальным методом реализации фишинговых атак являются фиш-киты — готовые наборы для создания фишинговых страниц. По данным исследования компании «Лаборатория Касперского» с октября 2022 по март 2023 года было обнаружено 2,5 миллиона уникальных фишинговых URL-адресов, сгенерированных с помощью фиш-китов. Данное программное обеспечение распространяется через Telegram-ботов, используя которые, злоумышленники могут создавать примитивные копии страниц популярных сервисов для кражи учётных данных. Также злоумышленники используют Telegram не только для распространения фиш-китов, но и для предоставления сервисов в рамках модели «фишинг как услуга» (phishing-as-a-service), в который могут включаться не только классические фишинговые инструменты, но и различные инструкции, а также техническая поддержка [2].

Именно методом генерации поддельных веб страниц воспользовались злоумышленники, запустившие новую фишинговую компанию, направленную против американских граждан, в ходе которой была размещена поддельная фишинговая страница почтовой службы USPS. По мнению экспертов по кибербезопасности компании Malwarebytes целью атаки являлось получение учётных данных жертв для входа в системы онлайн банкинга. Однако помимо поддельной фишинговой страницы, злоумышленники воспользовались новым методом обхода бдительности пользователей поискового сервиса Google, а именно проплаченное объявление, которое на первый взгляд имеет легитимный URL-адрес почтовой службы. Однако перейдя по ссылке из объявления потенциальные жертвы первоначально попадали на страницу, содержащие показатели объявления, а затем переадресовывались на фишинговый ресурс с поддельным доменным адресом. Особенностью данного вида атаки является обход классических методов визуализации фишинговой страницы в поисковом сервисе, что позволило злоумышленникам обмануть даже бдительных и информированных пользователей поискового сервиса [3].

Для защиты от подобных методов фишинга необходимо проявлять повышенную бдительность при использовании инструментов поисковых сервисов, а также не переходить по ссылкам из рекламных объявлений. Также эффективным методом будет использование блокировщиков рекламы на web страницах и визуальная проверка соответствия доменного имени сайта с официальным сайтом необходимой компании, а также SSL сертификата ресурса [4].

Фишинг также может использоваться как один из первых этапов многошаговой атаки для того, чтобы скомпрометировать учётные данные сотрудников организаций. Типичный пример фишинговой атаки — отправка письма по электронной почте с вредоносным сложением или ссылкой на фишинговый сайт. Однако спам-фильтры почтовых серверов успешно блокируют такие письма исходя из политик безопасности, а также из сигнатурных слов или выражений в теле письма. Исследователи из компании Inky зафиксировали актуальный способ распространения фишинговых писем, где злоумышленники обходили почтовые фильтры от спама и фишинга путём отправки электронных писем без текста, но с изображениями или QR-кодами. Целью преступников были учётные данные сотрудников различных организаций. Для успешной доставки письма злоумышленники использовали ранее скомпрометированные реальные адреса сторонних доменов. Вредоносный код был перемещён из тела письма в изображение, прикреплённое к письму, что, на данный момент, сильно затруднит автоматическое обнаружение такого рода фишинговых рассылок [5].

Методами защиты от такого вида фишинга могут быть: запрет вложений на почтовом сервере (при условии контроля сервера), разработка системы обнаружения вредоносной нагрузки в изображениях как модуль для антивирусной службы почтового сервера, использование специального программного обеспечения для проверки QR кодов и изображений на предмет вредоносного кода.

Наравне с перечисленными методами фишинга не теряет актуальности фишинг в социальных сетях и мессенджерах [6]. Злоумышленники могут комбинировать различные подходы, начиная от скомпрометированных учётных записей и заканчивая предложениями устроится на работу на выгодных условиях для соискателей. Мошенники зачастую злоупотребляют открытой информацией о потенциальной жертве. Открытый доступ к профилю социальной сети, небезопасные настройки конфиденциальности, а также публичный номер телефона в мессенджерах открывают дополнительные векторы атаки. Одним из самых опасных методов фишинга в социальных сетях и мессенджерах является адресный фишинг. Чаще всего такой вид мошенничества используется в крупных организациях и направлен сотрудников, занимаемых руководящие должности. Злоумышленники выдают себя за сотрудников организации, используя либо скомпрометированные учетные записи социальных сетей и мессенджеров, либо создают поддельные страницы, являющиеся копиями страниц реальных людей. Таким образом мошенники первоначально имеют повышенное доверие у невнимательных пользователей, которые могут предоставить им конфиденциальную или секретную информацию.

Для того, чтобы защититься от такого рода фишинговой атаки необходимо установить связь с тем человеком, который просит в социальных сетях конфиденциальные или иные данные доверенным способом, а именно каким-либо иным способом, чтобы идентифицировать являются ли адресатом такого рода запросов сотрудник организации, либо мошенник. Также необходимо сообщать о подобных инцидентах сотрудникам отдела информационной безопасности (или отдела информационных технологий) для инициации внутреннего расследования в том случае, если данные действия совершаются злоумышленниками.

Несмотря на постоянное усовершенствование механизмов защиты от различного типа фишинговых атак не стоит забывать, что такого рода атаки в первую очередь направлены на человека, а именно на его невнимательность или неосведомлённость. Также стоит отметить, что атакующие всё чаще используют различные настройки конфиденциальности сервисов в целях анонимизировать свою личность, а также обходят механизмы защиты актуальными методами реализации фишинговых атак.

Поэтому важно в совокупности с техническими методами защиты использовать методы повышения осведомлённости пользователей о различных методах реализации фишинговых атак.

В дальнейшей работе на основе систематизации методов фишинговых атак авторы планируют разработать новые и усовершенствовать имеющиеся средства расследования внутренних инцидентов информационной безопасности.

Исследование выполнено при частичной финансовой поддержке гранта Российского научного фонда (проект № 21–71–20078).

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В., Саенко И. Б., Чечулин А. А. Защита от нежелательной и вредоносной информации в глобальных информационных сетях // Информационно-психологическая и когнитивная безопасность: коллективная монография / под ред. И. Ф. Кефели, Р. М. Юсупова. СПб.: Изд-во «Аврора», 2017. С. 175–194.
2. «Лаборатория Касперского» проанализировала рынок фишинга в Telegram-каналах [Электронный ресурс]. URL: https://www.kaspersky.ru/about/press-releases/2023_laboratoriya-kasperskogo-proanalizirovala-rynok-fishinga-v-telegram-kanalah (дата обращения: 01.07.2023).
3. Google, почта США и неизвестная украинка: необычное трио фишинг-атаки [Электронный ресурс]. URL: https://www.securitylab.ru/news/539714.php (дата обращения 03.07.2023).
4. Комашинский Д.мВ., Котенко И.мВ., Чечулин А.мА. Категорирование веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Системы высокой доступности, 2011. Т. 7. № 2. С. 102-106.
5. Fresh Phish: Malicious QR Codes Are Quickly Retrieving Employee Credentials [Электронный ресурс]. URL: https://www.inky.com/en/blog/fresh-phish-malicious-qr-codes-are-quickly-retrieving-employee-credentials (дата обращения 06.07.2023).
6. Проноза А. А., Виткова Л. А., Чечулин А. А., Котенко И. В., Сахаров Д. В. Методика выявления каналов распространения информации в социальных сетях // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления, 2018. Т. 14. № 4. С. 362-377.

УДК 004

КОМПЛЕКСНЫЙ ПОДХОД К БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ВКЛЮЧАЯ ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

Грачев Михаил Иванович, Грачева Наталья Геннадьевна
Санкт-Петербургский университет МВД России
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: mig2500@mail.ru

Аннотация. В современном цифровом мире моделирование информационной безопасности предприятия может осуществляться через задействование программно-аппаратных средств, позволяющих осуществлять имитацию работы объекта, проверять и проводить его доработку в режиме реального времени. Одним из таких продуктов выступает программа AnyLogic позволяющая рассмотреть работу организации в виде тестовой модели.

Ключевые слова: предприятие, AnyLogic, информационная безопасность, обмен информацией, защищенность сети, управление, обмен данными.

INTEGRATED APPROACH TO ENTERPRISE SECURITY INCLUDING SIMULATION MODELING

Grachev Mikhail, Gracheva Natalya
SPIIRAS – SPCRAS
1 Pilot Pilyutova Av, St. Petersburg, 198206, Russia
e-mails: mig2500@mail.ru

Abstract. In the modern digital world, the modeling of information security of an enterprise can be carried out through the use of software and hardware that allow simulating the operation of an object, checking and completing it in real time. One of these products is the AnyLogic program, which allows you to consider the work of an organization in the form of a test model.

Keywords: enterprise, AnyLogic, information security, information exchange, network security, management, data exchange.

В современном мире происходят глобальные изменения. Эти изменения затронули и вопросы передачи информации между предприятиями и внутри предприятия. Информационные технологии внедряются в процессы жизнедеятельности организаций и человека. Влияние информационных технологий огромно, так как они позволяют обмениваться информацией на больших расстояниях, тем самым вопросы обеспечения информационной безопасности становятся всё более актуальной задачей.

Необходимо учесть, что к решению вопроса обеспечения информационной безопасности необходимо подходить комплексно. Комплекс мер направленных на обеспечение информационной безопасности будет состоять из решения задач по противодействию возникающим проблемам в системе управления для поддержания

штатной работы организации. Поддержание бесперебойной работы является важной задачей, решение которой отводится руководителю как лицу, принимающему решение.

Так как рассмотреть работу всех механизмов предприятия в комплексе является трудной задачей, зависящей от многих факторов, то нам может пригодиться программа имитационного моделирования AnyLogic позволяющая проводить системное рассмотрение. Соответственно, рассматривая организацию или предприятие необходимо декомпозировать рассматриваемый объект. В простом виде мы можем представить прямую зависимость от квалифицированного персонала (человеческий фактор) и технического оснащения (программно-аппаратный комплекс), которым располагает предприятие [1-3].

Многие исследователи отмечают проблему именно в человеческом факторе при обеспечении информационной безопасности [4-7]. В связи с этим зависимость бесперебойной работы предприятия от работы человека существенна. Имитационное моделирование предприятия с помощью программного комплекса AnyLogic позволяет решать вопрос по зависимости решения задач от потока событий и в последующем анализировать полученные действия [8].

Программа предназначена для исследования функционирования организации для оценки вероятностно временных характеристик выполнения основных функций с учетом возможного влияния угроз работе информационной системе организации, требующая выполнения определенных действий по выявлению и устранению воздействия угроз на информационную систему, с последующими действиями, направленными на бесперебойную работу [8].

Таким образом, для реализации мероприятий по предупреждению срывов в работе предприятия можно воспользоваться имитационным моделированием для предварительного расчета сложных ситуаций, которые могут возникнуть в работе предприятия [9, 10].

СПИСОК ЛИТЕРАТУРЫ

1. Бурлов В. Г., Грачев М. И., Примакин А. И. О необходимости подготовки и переподготовки квалифицированных кадров в сфере безопасности информационных технологий // Информационная безопасность регионов России (ИБРР-2017) : Материалы конференции, Санкт-Петербург, 01–03 ноября 2017 г. СПб : СПОИСУ, 2017. С. 470-472. EDN HFJEXS.
2. Бурлов В. Г., Грачев М. И., Примакин А. И. Многоуровневый подход в подготовке и переподготовке кадров в сфере безопасности информационных технологий // Региональная информатика и информационная безопасность : сборник научных трудов, Санкт-Петербург, 01–03 ноября 2017 г. Выпуск 3. СПб : СПОИСУ, 2017. С. 185-189. EDN YNAEGV.
3. 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-Петербург, 26–28 октября 2016 г. Выпуск 2. СПб : СПОИСУ, 2016. С. 80-84. EDN XEYLMF.
4. Скворцов И. П., Титарев А. О. О проблеме человеческого фактора в обеспечении информационной безопасности // Воздушно-космические силы. Теория и практика. 2022. № 23. С. 106-113. EDN HYFMVI.
5. Калуцкий И. В., Агафонов А. А. Роль человеческого фактора в обеспечении информационной безопасности бизнеса // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2012. № 2-2. С. 173-178. EDN RDGWMT.
6. Трошин Д. В. Безопасность предприятия: смысл, онтология, оценка. Тверь : Тверской государственный университет, 2015. 212 с. ISBN 978-5-7609-1048-6. EDN UQUZUX.
7. Золотова В. А. Направления развития интеллектуальной информационной технологии прогнозирования состояния предприятий промышленности России в условиях неблагоприятных внешних воздействий // 2022. № 4(86). С. 71-78. DOI 8.17277/voprosy.2022.04. Pp. 071-078. EDN LCDRXT.
8. Грачев М. И., Бурлов В. Г., Захаров И. С., Чудаков О. Е. Свидетельство о государственной регистрации программы для ЭВМ № 2021614433, РФ. Обобщенная имитационная модель функционирования системы управления высшим учебным заведением : № 2021611990 : заявл. 16.02.2021 : опубл. 24.03.2021. EDN NFBBLM.
9. Грачев М. И. Имитационное моделирование процессов управления // Интеллектуальные системы в производстве. 2022. Т. 20, № 4. С. 64-71. DOI 10.22213/2410-9304-2022-4-64-71. EDN JHVVWR.
10. Грачев М. И., Бурлов В. Г., Чудаков О. Е., Примакин А. И. Имитационная модель управления образовательной организацией высшего образования // XXI век: итоги прошлого и проблемы настоящего плюс. 2021. Т. 10, № 1(53). С. 57-62. DOI 10.46548/21vek-2021-1053-0010. EDN BJCEUH.

УДК 004.056

АНАЛИЗ УСЛОВИЙ МОДЕЛИРОВАНИЯ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ В ИНДУСТРИАЛЬНЫХ СИСТЕМАХ ОЧИСТКИ ВОДЫ

Десницкий Василий Алексеевич
Федеральное государственное бюджетное учреждение науки
СПИИРАН – СПб ФИЦ РАН
14 линия ВО, 39, Санкт-Петербург, 199178, Россия
e-mail: desnitsky@comsec.spb.ru

Аннотация. Работа ориентирована на решение задач по анализу выполнимости атакующих воздействий в индустриальных системах очистки воды и обнаружению атак в них. Проводится анализ факторов риска нелегитимной работы системы и выбор программно-аппаратных сенсоров, которые могут быть встроены в лабораторный стенд для решения задач обнаружения актуальных видов нелегитимных воздействий.

Ключевые слова: моделирование, атака, система очистки воды.

ANALYSIS OF MODELING CONDITIONS OF ATTACKS IN INDUSTRIAL WATER PURIFICATION SYSTEMS

Desnitsky Vasily
SPIIRAS – SPCRAS
39, 14-th Linia, St. Petersburg, 199178, Russia
e-mail: desnitsky@comsec.spb.ru

Abstract. The work is targeted on problems of analyzing the feasibility of attacks in industrial water purification systems and detecting attacks in them. An analysis of the risk factors for illegitimate operation of the system and software/hardware sensors choice that can be embedded into a laboratory test-bench to solve the problems of detecting relevant types of illegitimate impacts on the system elements are performed.

Keywords: modeling, attack, detection, water purification system.

Работа направлена на решение задач анализа и повышения защищенности индустриальных автоматизированных систем очистки воды. Проблема повышения защищенности таких систем обусловлена рядом факторов, включающих ограниченность нормативов в данной предметной области, недостаточность учета вопросов информационной безопасности на стадии проектирования таких систем, а также вариативность действий потенциального злоумышленника, пытающегося скомпрометировать такую систему, отдельные ее устройства и компоненты, нарушить достоверность циркулирующих в ней данных и корректность функционирования предоставляемых ею сервисов.

Исследование ориентировано на применение разрабатываемых средств обнаружения атак в рамках двух испытательных лабораторных стендов водоочистки индустриального уровня [1], включающих, во-первых, процессы механической очистки воды, во-вторых, процессы биологической очистки, и, в-третьих, физико-химические процессы очистки.

В работе анализируется ряд факторов риска нелегитимной работы системы, а также виды программно-аппаратных сенсоров, которые могут быть встроены в лабораторный стенд для решения задач обнаружения соответствующих им нелегитимных воздействий [2]. В частности, фактор отказа насоса подачи сырой воды сопряжен с использованием датчика потока воды с отслеживанием его срабатываний во времени в течение определенного периода. Такой датчик позволяет непосредственно фиксировать процесс функционирования насоса и его особенности [3]. Для обнаружения несанкционированного отсутствия перемешивания сырой воды предлагается использование дальномера, позволяющего фиксировать неработоспособность и неподвижность конструкций перемешивателя. Также возможно перехватывать управляющий электрический сигнал, подаваемый на перемешиватель, и по фактически потребляемой им мощности отслеживать работоспособность элемента. Кроме того, несанкционированное отсутствие перегородок в резервуаре флоктуации может быть выявлено также при помощи дальномера с использованием пары встраиваемых меток RFID или NFC, одна из которых подвешивается на перегородку, а вторая — на сканер на стационарной конструкции рядом.

Результаты анализа факторов рисков нелегитимной работы системы водоочистки предполагается использовать как основу для формирования набора программно-аппаратных сенсоров, которые могут быть встроены в используемые лабораторные стенды для снятия первичных данных для обнаружения актуальных видов атак на такие системы.

Работа выполняется в СПб ФЦ РАН при финансовой поддержке проекта Российского научного фонда № 23-11-20024.

СПИСОК ЛИТЕРАТУРЫ

1. Al-Dhaheri M., Zhang P., Mikhaylenko D. Detection of Cyber Attacks on a Water Treatment Process // IFAC-PapersOnLine. Vol. 55. Iss. 6. 2022. P. 667-672.
2. Meleshko A. V., Desnitsky V. A., Kotenko I. V. Machine learning based approach to detection of anomalous data from sensors in cyber-physical water supply systems // IOP Conference Series: Materials Science and Engineering. International Conference on Modern Trends in Manufacturing Technologies and Equipment 2019, ICMTME 2019. 2020. Paper number. 033034.
3. Desnitsky V., Kotenko I. Monitoring the state of materials in cyberphysical systems: water supply case study // Materials Today: Proceedings. 2019. P. 410-416.

УДК 004.056

ОБНАРУЖЕНИЕ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ НА ОСНОВЕ ГРАФО-ОРИЕНТИРОВАННОГО МОДЕЛИРОВАНИЯ СОСТОЯНИЙ СИСТЕМЫ

Десницкий Василий Алексеевич
СПИИРАН – СПб ФИЦ РАН
14 линия В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: desnitsky@comsec.spb.ru

Аннотация. В работе предложен подход к обнаружению атакующих воздействий в критически важных инфраструктурах Интернета вещей с применением методов графо-ориентированного моделирования и машинного обучения. В подготовительном режиме производится интеллектуальный анализ исходных данных о функционировании индустриальной системы с использованием кластеризации возможных состояний системы, а также построение графа ее состояний и переходов. На этапе выполнения проводится обход графа с последовательным выявлением состояний, описывающих присущие системе атаки определенных классов.

Ключевые слова: моделирование, атака, обнаружение, информационная безопасности.

DETECTION OF ATTACKS ON GRAPH-BASED MODELING OF SYSTEM STATES

Desnitsky Vasily
SPIIRAS – SPCRAS
39 14-th Linia, St. Petersburg, 199178, Russia
e-mail: desnitsky@comsec.spb.ru

Abstract. The work proposes an approach to detecting attacks in critical infrastructures of the Internet of Things by using graph-based modeling and machine learning methods. In the primary mode, an intellectual analysis of the initial data on the functioning of the industrial system is performed through using the clustering of possible states of the system, as well as the construction of a graph of its states and transitions. At the runtime stage, the graph is traversed with sequential identification of states that describe the attacks of certain classes inherent in the system.

Keywords: modeling, attack, detection, information security.

Критически важный характер современных систем Интернета вещей, таких как транспортных и энергетических систем, систем имплантируемых медицинских устройств, систем управления водоснабжением Умного города, определяет высокую актуальность научно-технической задачи обнаружения киберфизических атак в таких системах [1]. Успешное осуществление шагов атаки, как со стороны внешнего, так и внутреннего нарушителя, могут привести к значительным нарушениям в работе таких систем, серьезному материальному ущербу и даже к катастрофическим последствиям для инфраструктуры системы и ее окружения. Все это обусловливает формирование научно-технической задачи по разработке способов обнаружения атак на такие системы, в том числе путем построения новых, автоматизации и интеллектуализации имеющихся компонентов обнаружения атак на основе графов.

Проведен анализ релевантных работ в предметной области моделирования и обнаружения атак в критически важных системах, а также рассмотрен ряд наборов данных, описывающих возможные перечни показаний программных сенсоров таких систем [2]. На основе применения метода birch-кластеризации и выбора принятого за оптимальное порогового значения с использованием индексов Калински-Харабаса и Дэвиса-Булдина проводится автоматизированное агрегирование фактических состояний системы в некоторый ограниченный набор состояний. При этом каждое агрегированное состояние будет представляться некоторой вершиной графа состояний и переходов. Разработанный граф включает нормальные состояния системы, а также атакующие состояний, причем каждое состояние может быть либо нормальным, либо атакующим. Вместе с тем атакующее состояние может включать несколько видов атак, выполняемых нарушителем параллельно. Построение матрицы переходов осуществляется между состояниями путем применения скользящего временного окна длиной H=3600 событий с шагом t=60 событий и вычисления среднего количества появлений двух последовательных состояний. Построенный алгоритм обхода графа позволяет динамически отслеживать факт достижения атакующих состояний системы и, в случае достижения такого состояния, сигнализировать о типе атаки, ее источнике и других ее характеристиках.

Проведенные эксперименты с использованием программного модуля, реализующего предложенный подход к обнаружению атак на базе набора данных Electra [3], показали, во-первых, высокие значения показателей точности и полноты обнаружения атак, и, во-вторых, высокую устойчивость разработанного алгоритма обнаружения атак к потерям поступающих пакетов с данными об анализируемых показаниях сенсоров системы.

СПИСОК ЛИТЕРАТУРЫ

1. Desnitsky V. A., Kotenko I. V. Security event analysis in XBee-based wireless mesh networks // Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2018. Pp. 42-44.
2. Desnitsky V., Kotenko I., Zakoldaev D. Evaluation of resource exhaustion attacks against wireless mobile devices // Electronics. 2019. Vol. 8. № 5. Article number. 500.
3. On the generation of anomaly detection datasets in industrial control systems / Gómez Á. L. P., Maimó L. F., Celdrán A. H. [et al] // IEEE Access. Vol. 7, 2019. Pp. 177460-177473.

УДК 004.056

РЕПУТАЦИОННО-ДОВЕРИТЕЛЬНЫЕ МОДЕЛИ ДЛЯ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ НА ОСНОВЕ БЛОКЧЕЙНА

Донсков Евгений Андреевич, Котенко Игорь Витальевич
СПИИРАН – СПб ФИЦ РАН
14-я линия В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: radion2002@gmail.com, ivkote@comsec.spb.ru

Аннотация. В настоящее время репутационно-доверительные модели широко применяются в информационной безопасности для решения задачи поиска злоумышленников. В работе рассматриваются актуальные репутационно-доверительные модели для интеллектуальных транспортных систем на основе блокчейна или для составляющих компонентов подобной системы.

Ключевые слова: информационная безопасность; репутационно-доверительная модель; интеллектуальные транспортные системы; распределенный реестр; блокчейн.

REPUTATION AND TRUST MODELS FOR INTELLIGENT TRANSPORT SYSTEMS BASED ON BLOCKCHAIN

Donskov Evgenii, Kotenko Igor
SPIIRAS – SPCRAS
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: radion2002@gmail.com, ivkote@comsec.spb.ru

Abstract. Currently, reputation-trust models are widely used in information security to solve the problem of finding intruders. The paper discusses current reputation and trust models for intelligent transport systems based on blockchain or for components of a similar system.

Keywords: information security; reputation and trust model; intelligent transport systems; distributed registry; blockchain.

Важнейшей задачей при проектировании сложных информационно-телекоммуникационных систем, к классу которых относятся интеллектуальные транспортные системы на основе блокчейна, является обеспечение информационной безопасности [1]. Одним из перспективных классов моделей, используемых для обеспечения информационной безопасности, являются репутационно-доверительные модели. Разработка моделей, обеспечивающих оценку рейтинга устройства, объекта или целого приложения относится к актуальному направлению исследований в области информационной безопасности систем и служит для определения возможности доверия и обмена данными с ним [2]. В рамках интеллектуальной транспортной системы на основе блокчейна подобный инструмент предоставляет особый интерес, так как это позволяет решить общую задачу — классификацию валидных пользователей и злоумышленников, что является одной из важнейших составляющих для обеспечения безопасности системы.

Репутационно-доверительные модели помогают предотвратить потенциально опасные ситуации, улучшить безопасность и даже установить контроль над доступом к объектам [3]. Они поощряют честное поведение и снижают вероятность возникновения мошенничества, угроз и других преступных действий.

Одной из проблем, связанных с репутационно-доверительными математическими моделями является их несовершенство и различия в вычислении доверия и репутации [4]. Также могут возникать проблемы с обработкой большого количества данных, вопросы конфиденциальности и защиты данных пользователей интеллектуальной транспортной системы на основе блокчейна [5]. В работе рассмотрены репутационно-доверительные модели для интеллектуальных транспортных систем на основе блокчейна или для составляющих компонентов подобной системы. В дальнейшем исследования будут направлены на улучшение репутационно-доверительных моделей, включая разработку новых методов и алгоритмов, которые учитывают особенности применения в интеллектуальных транспортных системах на основе блокчейна.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В., Десницкий В. А., Чечулин А. А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд, 2011. № 3. С.68-75.
2. Зикратов И. А., Зикратова Т. В., Лебедев И. С., Гуртов А. В. Построение модели доверия и репутации к объектам мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2014. №3 (91). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/postroenie-modeli-doveriya-i-reputatsii-k-obektam-multiagentnyh-robototehnicheskih-sistem-s-detsentralizovannym-upravleniem (дата обращения: 05.07.2023).
3. Zishen S., Jie P., Lingyu J., Fazhuan W., Dong W. A Reputation-based Dynamic Trust Model in P2P E-commerce Environment // China Automation Congress (CAC), Beijing, China, 2021. Pp. 6432-6438, doi: 10.1109/CAC53003.2021.9727778.
4. Najib W., Sulistyo S., Widyawan. Survey on Trust Calculation Methods in Internet of Things // Procedia Computer Science. Jan. 2019. Vol. 161. Pp. 1300-1307.
5. Peiris P. P. C., Rajapakse C., Jayawardena B. Blockchain-based distributed reputation model for ensuring trust in mobile adhoc networks // International Research Conference on Smart Computing and Systems Engineering (SCSE). Colombo, Sri Lanka, 2020. Pp. 51-56, doi: 10.1109/SCSE49731.2020.9312998.

УДК 004.451:004.056

БЕЗОПАСНАЯ ТЕХНОЛОГИЯ ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Дубенецкий Владислав Алексеевич, Кузнецов Александр Григорьевич, Цехановский Владислав Владимирович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
e-mails: dubvl@list.ru, agkuznetcov@etu.ru, vvcehanovsky@mail.ru

Аннотация. Предлагается безопасная технология проектирования информационных систем на основе анализа шаблонов. Для построения информационной модели системы в методике используется унифицированный язык моделирования (UML).

Ключевые слова: унифицированный язык моделирования UML; информационная система; расширенный язык SQL; объектная модель предметной области; объектно-ориентированное моделирование.

SAFE DESIGN TECHNOLOGY INFORMATION SYSTEMS

Dubenetsky Vladislav, Kuznetsov Alexander, Tsekhanovsky Vladislav
St. Petersburg State Electrotechnical University «LETI» named after. V. I. Ulyanova (Lenin)
5 Professora Popova St., St. Petersburg, 197022, Russia
e-mails: dubvl@list.ru, agkuznetcov@etu.ru, vvcehanovsky@mail.ru

Abstract. A secure technology for designing information systems based on pattern analysis is proposed. To build an information model of the system, the methodology uses a unified modeling language (UML).

Keywords: unified modeling language UML; information system; advanced SQL language; domain object model; object-oriented modeling.

Для описания объектной модели предметной области будем использовать UML (Unified Modeling Language). Известно, что язык UML поддерживает объектно-ориентированное моделирование и предоставляет достаточный набор возможностей для описания различных аспектов предметной области.

Модели прецедентов, классов, состояний, поведения позволяют в полной мере описать онтологию предметной области, функциональные требования к приложению, проектные решения в виде строгих спецификаций.

Интерес представляет не столько графическая форма языка, сколько семантика объектного моделирования.

Использование шаблонов как источников для построения модели предъявляет другие требования к правилам анализа компонентов документов:

модель должна отражать не структуру шаблона, а первичные взаимосвязи между объектами предметной области, исключая избыточность описания. Поэтому при анализе содержания каждого компонента шаблона требуется выделять:

– базовые классы предметной области,
– отношения обобщения/конкретизации,
– выделять в шаблоне вторичные роли,
– находить истинные классы для аргументов выявленных ролей.

Тексты, представленные в шаблонах, сопровождающих хозяйственную деятельность, в отличие от литературных текстов, содержат формализованные данные, понимание которых в сильной степени связано с контекстом деятельности. По этой причине прямой лингвистический анализ содержания шаблона затруднен. При анализе приходится формировать предложения с использованием текстов компонентов и добавления фрагментов предложения, принятых по умолчанию.

Неправильный выбор архитектурных решений может привести к тому, что проектируемая система станет заказной с оригинальными метаданными и кодом реализации. Кроме того, классические решения приводят к тому, что модель домена предметной области, претерпевающая изменения, растворяется в коде приложения.

Одним из направлений разрешения проблем неправильного выбора архитектурных решений и искажения модели домена предметной области, является применение технологии проектирования, основанной на использовании моделей, допускающих исполнение.

СПИСОК ЛИТЕРАТУРЫ

1. Рамбо Дж., Якобсон А., Буч Г. UML. Специальный справочник. СПб.: Питер, 2002. 656 с.
2. Рамбо Дж., Баха М. UML 2/0/ Объектно-ориентированное моделирование и разработка. 2-е изд. СПб.: Питер, 2007. 544 с.
3. Дубенецкий В. А., Советов Б. Я., Цехановский В. В. Проектирование корпоративных информационных систем. СПБ: Изд-во СПбГЭТУ «ЛЭТИ», 2013. 189 с.
4. Основы использования XML Schema для определения элементов [Электронный ресурс]. URL: http://iso.ru/ru/press-center/journal/1725.phtml. (дата обращения: 31.07.2023).

УДК 004.8

МОДЕЛЬ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ ДЛЯ ВИЗУАЛЬНОГО АНАЛИЗА ДАННЫХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Жернова Ксения Николаевна
СПИИРАН – СПб ФИЦ РАН
14-я линия В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: zhernova@comsec.spb.ru

Аннотация. Искусственные нейронные сети являются вспомогательным инструментом для всестороннего анализа различных данных во многих сферах науки и технологии. В том числе нейронные сети используются в области информационной и компьютерной безопасности, например, при разработке всевозможных методов биометрической аутентификации. Однако данная технология может быть полезна и в других направлениях информационной безопасности, таких как визуальный анализ данных безопасности. До недавнего времени считалось, что визуальный анализ должен проводиться человеком-оператором. В данном докладе показано, что нейронная сеть также способна с высокой точностью определять, присутствует ли аномалия на изображении данных безопасности.

Ключевые слова: искусственные нейронные сети, машинное обучение, компьютерное зрение, информационная безопасность, визуальный анализ, визуализация данных.

ARTIFICIAL NEURAL NETWORK MODEL FOR VISUAL ANALYSIS OF INFORMATION SECURITY DATA

Zhernova Ksenia
SPIIRAS – SPCRAS
39 14 Line, St. Petersburg, 199178, Russia
e-mails: zhernova@comsec.spb.ru

Abstract. Artificial neural networks are an auxiliary tool for comprehensive analysis of various data in many areas of science and technology. Moreover, neural networks are used in the field of information and computer security, for example, in the development of various methods of biometric authentication. However, this technology can be useful in other areas of information security, such as visual analysis of security data. Until recently, it was believed that visual analysis should be carried out by a human operator. This report shows that the neural network is also able to determine with high accuracy whether an anomaly is present in the image of security data.

Keywords: artificial neural networks, machine learning, computer vision, information security, visual analysis, data visualization.

В последнее время разрабатывается большое количествомоделей свёрточных нейронных сетей, позволяющих анализировать изображения. Данная технология применяется во многих областях науки и человеческой деятельности. Однако существует мало исследований, посвящённых анализу данных, визуализированных в виде диаграмм, в то время как визуальный анализ — неотъемлемая часть информационной безопасности [1]. Ниже описана модель нейронной сети, которая позволит совершать поиск аномалий на визуализации данных безопасности.

Для проектирования модели использовалась библиотека Pytorchязыка Python. Слои предложенной модели нейронной сети были расположены в следующем порядке: Conv2D (с функцией активации relu), BatchNorm2d, MaxPool2d, Conv2D (активация relu), BatchNorm2d, MaxPool2d, Conv2D (активация relu), BatchNorm2d, Dropout, MaxPool2d, Conv2D, Dropout, Flatten, Linear, Dropout, Linear (активация log_softmax). Ниже представлены краткие описания для каждого типа использованного слоя [2].

– Conv2D — свёрточныйслой, необходимый для работы нейронной сети с изображениями. В использованной библиотеке Pytorch этот слой можно объединять с функцией активации relu.

– MaxPool2d — данный слой позволяет снизить количество необходимых для обучения признаков.

– Dropout — слой, отбрасывающий случайные нейроны, что в некоторых случаях позволяет повысить эффективность модели нейронной сети.

– BatchNorm2d — данный слой нормализует среднее значение скрытых слоёв, а также распределение их значений [3].

– Flatten — слой, использующийся для того, чтобы сделать данные пригодными для проведения над ними линейных преобразований.

– Linear используется для линейного преобразования поступающих данных.

Для того, чтобы рассчитать показатель потерь при обучении, была задействована функция CrossEntropyLoss [2].

Функция активации необходима для того, чтобы внести нелинейность при обучении [2]. С этой целью вместе со свёрточными слоями была использована функция активации relu. Данная функция является одной из самых эффективных с точки зрения скорости. Кроме того, в свёрточных нейронных сетях чаще всего применяют именно её. Активация на выходе была произведена с помощью фукциилog_softmax, поскольку она является одной из наиболее стабильных при получении значения потерь [2].

Данная модель в процессе обучения на 10000 изображений при прохождении 12 эпох позволила достичь максимального возможного показателя по тренировочной точности (trainaccuracy) итестовой точности (validationaccuracy), в обоих случаях принимая значение 100%. В качестве модели визуализации был взят часто использующийся в области информационной безопасности график Scatterplot.

В докладе представлена архитектура модели искусственной нейронной сети, которая позволяет точно классифицировать визуализированные данные безопасности по группам: аномальные и не аномальные данные. Данная модель может быть полезна для автоматизации поиска аномалий в графически представленных данных безопасности и может найти применение в системах информационной и компьютерной безопасности.

Работа выполнена при финансовой поддержке РНФ (проект 21-71-20078).

СПИСОК ЛИТЕРАТУРЫ

1. Коломеец М. В., Чечулин А. А., Дойникова Е. В., Котенко И. В. Методика визуализации метрик кибербезопасности // Изв. вузов. Приборостроение, Т. 61, № 10, 2018, С. 873-880. DOI: 10.17586/0021-3454-2018-61-10-873-880.
2. Torch.nn — Pytorch 2.0 documentation. 2023. [Электронный ресурс]. URL: https://pytorch.org/docs/stable/nn.html (last accessed 02.07.2023).
3. Sergey I., Christian S. Batch normalization: Accelerating deep network training by reducing internal covariate shift, 2015 // arXiv: 1502.03167v3 [cs.LG]. https://doi.org/10.48550/arXiv.1502.03167.

УДК 004.8

ПРОБЛЕМЫ ВИЗУАЛЬНОГО АНАЛИЗА ДАННЫХ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Жернова Ксения Николаевна
СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: zhernova@comsec.spb.ru

Аннотация. Искусственные нейронные сети получают всё большее распространение и начинают применяться в различных направлениях научной и коммерческой деятельности, таких как экономика, медицина и анализ больших данных. Также нейронные сети находят применение и в компьютерной безопасности, однако с визуализацией данных работает оператор-человек. При большом объёме визуализированных данных работа оператора-человека может быть затруднена. Данное исследование направлено на выявление работ по использованию искусственных нейронных сетей для визуального анализа событий безопасности. В докладе будет проведён обзор исследований, рассматривающих работу искусственных нейронных сетей с визуализацией данных, а также показана нехватка исследований в области визуального анализа данных нейронной сетью в области информационной безопасности.

Ключевые слова: искусственные нейронные сети, машинное обучение, компьютерное зрение, информационная безопасность, визуальный анализ, визуализация данных.

PROBLEMS OF VISUAL ANALYSIS OF DATA IN THE FIELD OF INFORMATION SECURITY USING ARTIFICIAL NEURAL NETWORKS

Zhernova Ksenia
SPIIRAS – SPCRAS
39 14 Liniya, St. Petersburg, 199178, Russia
e-mails: zhernova@comsec.spb.ru

Abstract. Artificial neural networks are becoming more widespread and they are beginning to be used in various areas of scientific and commercial activities, such as economics, medicine, and big data analysis. Moreover, neural networks are used in computer security, however, a human operator works with data visualization. With a large amount of visualized data, the work of a human operator can be difficult. This study aims to identify papers on the use of artificial neural networks for visual analysis of security events. The report will review the research on the work of artificial neural networks with data visualization, and it will also show the lack of research in the field of visual data analysis by a neural networkin the field of information security.

Keywords: artificial neural networks, machine learning, computer vision, information security, visual analysis, data visualization.

Несмотря на практически повсеместное использование искусственных нейронных сетей, в том числе в области информационной безопасности, всё ещё требуется контроль оператора-человека. Однако применение нейронных сетей позволяет автоматизировать многие сферы человеческой деятельности, такие как распознавание текста, анализ биометрических данных, и т.п. Также нейронные сети могли бы найти применение и в области визуального анализа событий безопасности, представленных в виде различных графиков и схем, применяющихся для представления данных безопасности [1].

В рамках данного исследования был изучен ряд современных работ, которые можно распределить по трём условным группам в зависимости от способа применения искусственной нейронной сети при работе с визуализацией данных:

(1) оценка работы нейронной сети;
(2) визуализация данных;
(3) визуальный анализ данных.

Данные группы будут более подробно описаны ниже.

Оценка работы нейронной сети. В данную категорию вошли работы, описывающие способы применения визуализации для отображения эффективности работы нейронной сети. Например, с помощью таких визуализаций можно оценивать, насколько правильно подобраны параметры модели нейронной сети [2]. Также визуализацию можно использовать для того, чтобы оценить точность выполнения нейронной сетью поставленной задачи [3]. Кроме того, визуализация может использоваться для демонстрации признаков, которые нейронная сеть была обучена распознавать [4].

Визуализация данных. Данная группа содержит исследования по разработке моделей визуализации с помощью нейронных сетей. Существуют работы, в которых нейронная сеть сама визуализирует данные [5]. Также нейронные сети оказались способны предлагать наиболее релевантные модели визуализации из имеющихся и предлагать их оператору в зависимости от выполняемой им задачи [6].

Визуальный анализ данных. Данная группа предполагает работы, исследующие анализ изображений с помощью нейронных сетей. Основная масса работ была посвящена анализу различных изображений. На данных изображениях производился поиск конкретных объектов, например, вооружённых людей [7]. Также

может производиться классификация изображений, исходя из определённых признаков. Например, диагностика болезни Альцгеймера по снимкам головного мозга [8].

Третья группа представляет особенный интерес для данного исследования, так как данное направление позволило бы автоматизировать визуальный анализ данных безопасности. Данная группа является малочисленной, что показывает недоисследованность области. При этом в ней не были выявлены работы, направленные на использование компьютерного зрения для поиска аномалий в событиях безопасности.

В докладе представлен краткий обзор существующих работ по теме визуального анализа данных безопасности средствами искусственных нейронных сетей. Выявлена проблема нехватки исследований, касающихся визуального анализа данных иинформационной безопасности с применением нейронных сетей. На основе данного исследования можно сделать вывод о том, что существующие работы практически не затрагивают тему визуального анализа данных безопасности с помощью нейронных сетей. Однако применение моделей свёрточных нейронных сетей, используемых для классификации изображений и обнаружения объектов на изображении, может быть обосновано в системах принятия решенийдля автоматизации анализа поведения траффика на предмет возможных аномалий.

Работа выполнена при финансовой поддержке РНФ (проект 21-71-20078).

СПИСОК ЛИТЕРАТУРЫ

1. Коломеец М. В., Чечулин А. А., Дойникова Е. В., Котенко И. В. Методика визуализации метрик кибербезопасности // Изв. вузов. Приборостроение, Т. 61. № 10, 2018, С. 873-880. DOI: 10.17586/0021-3454-2018-61-10-873-880.
2. Park H., Nam Y., Kim J. H., Choo J., HyperTendril: Visual analytics for user-driven hyperparameter optimization of deep neural networks // IEEE Transactions on Visualization and Computer Graphics. Vol. 27. No. 2. Pp. 1407-1416, 2020.
3. Bilal A., Jourabloo A., Ye M., Liu X., Ren L. Do convolutional neural networks learn class hierarchy? // IEEE transactions on visualization and computer graphics. Vol. 24. № 1. Pp. 152-162, 2017.
4. Smooth grad-cam++: An enhanced inference level visualization technique for deep convolutional neural network models / Omeiza D. [et al.] // arXiv preprint arXiv:1908.01224. 2019.
5. Medvedev V., Dzemyda G., Kurasova O., Marcinkevičius V., Efficient data projection for visual analysis of large data sets using neural networks // Informatica. Vol. 22. № 4. Pp. 507-520, 2011.
6. Zhao J., Fan M., Feng M. Chartseer: Interactive steering exploratory visual analysis with machine intelligence // IEEE Transactions on Visualization and Computer Graphics. Vol. 28. № 3. Pp. 1500-1513, 2020.
7. Torres M., Cantú F. Learning to see: Convolutional neural networks for the analysis of social science data. Political Analysis. Vol. 30. №. 1. Pp. 113-131. 2022.
8. Classification and visualization of Alzheimer's disease using volumetric convolutional neural network and transfer learning / Oh K. [et al.] // Scientific Reports. 2019. Vol. 9. №. 1. DOI:10.1038/s41598-019-54548-6.

УДК 004.056

АНАЛИЗ МЕТОДОВ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ, ПРИМЕНЯЕМЫХ ДЛЯ ОБНАРУЖЕНИЯ МНОГОШАГОВЫХ КИБЕРАТАК

Зеличенок Игорь Юрьевич, Котенко Игорь Витальевич
СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: zelichenok@comsec.spb.ru, ivkote@comsec.spb.ru

Аннотация. В связи с возрастанием объема данных и увеличением сложности объектов защиты, многошаговые кибератаки становятся все более распространенными и сложно обнаруживаемыми. В докладе рассматриваются основные методы, используемые для обнаружения многошаговых атак на основе технологий больших данных, а также обсуждаются преимущества и недостатки каждого метода. Дается представление о текущей реализации прототипа системы обнаружения многошаговых кибератак на основе технологий больших данных.

Ключевые слова: кибербезопасность; big data; многошаговые кибератаки; обнаружение атак.

ANALYSIS OF BIG DATA PROCESSING METHODS USED TO DETECT MULTI-STEP CYBER ATTACKS

Zelichenok Igor, Kotenko Igor
SPIIRAS – SPCRAS
39 14th line Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: zelichenok@comsec.spb.ru, ivkote@comsec.spb.ru

Abstract. Due to the increase in the volume of data and the growth in the complexity of the protection objects, multi-step cyber-attacks are becoming more common and difficult to detect. The work reviews the main methods used to detect multi-step attacks based on big data technologies, and discusses the advantages and disadvantages of each method. An idea is given of the current implementation of a prototype system for detecting multi-step cyber-attacks based on big data technologies.

Keywords: cyber security; big data; multi-step cyber-attacks; attack detection.

В настоящее время с появлением новых технологий и сетевых угроз стало ясно, что обнаружение многошаговых атак является одной из ключевых задач в области кибербезопасности [1]. Традиционные методы

обнаружения атак зачастую неспособны эффективно распознавать сложные многоэтапные атаки, которые искусно маскируются и распространяются внутри защищаемой системы на протяжении продолжительного времени.

С целью решения этой проблемы и повышения эффективности обнаружения многошаговых атак в последние годы было разработано множество подходов, основанных на технологиях больших данных (Big Data) [2]. Обработка больших данных представляет собой задачу анализа и обработки огромных объемов информации, генерируемых различными источниками данных, такими как логи сетевого трафика, системные журналы и другие событийные данные [3].

Для обработки больших данных, не требующих своевременного реагирования, применяется пакетная обработка [4, 5] больших данных. При использовании данного метода данные собираются в пакеты (batch) и сохраняются. После чего пакет пересылается далее и обрабатывается.

Потоковая обработка данных позволяет получать информацию о защищаемой системе в реальном времени, что позволяет своевременно реагировать на поступающие угрозы. Такой подход распространен при обработке данных с датчиков, логов событий, транзакций и др. [6]. Этот метод позволяет обрабатывать данные в потоке, не сохраняя их на диске, что позволяет сократить задержки и ускорить обработку данных [7, 8].

Суть метода MapReduce заключается в параллельной обработке больших данных на кластерах серверов [9, 10]. Метод основан на применении двух процедур: во время операции map данные разделяются и обрабатываются на узлах кластера, на втором же этапе данные группируются по критериям, что позволяет сократить изначальный объем.

Помимо методик оптимизации потоков больших данных также используются вспомогательные способы для ускорения обработки. Например, избегание взаимодействия с файловой системой при помощи обработки данных в оперативной памяти. Однако, такой метод требует большого объема ОЗУ на сервере [11, 12].

Нередко скорость обработки повышают при помощи баз данных NoSQL. В отличии от реляционных баз данных, они не требуют фиксированной схемы данных и позволяют более гибкое хранение разнородных данных. Вместо таблиц данные могут быть организованы в коллекции, документы, графы или столбцы. NoSQL базы данных обеспечивают высокую горизонтальную масштабируемость [13, 14], то есть возможность расширения базы данных на несколько серверов.

Использование машинного обучения в Big Data позволяет ускорить обработку за счет автоматического извлечения знаний [15] и принятия решений [16], однако методы машинного обучения требуют большого объема размеченных данных для обучения и обновления моделей при изменении данных.

Для реализованного прототипа было принято решение использовать комбинированные методы пакетной и потоковой обработки вместе с NoSQL базой данных и обработкой данных внутри оперативной памяти.

Компоненты сбора обрезают нерелевантные данные, затем передают поток событий на сервер-обработчик по http-протоколу. При перегрузке сервера данные о поведении защищаемого узла сети собираются в пакеты на стороне агента и отсылаются на сервер. Такой метод позволяет снизить частоту передачи данных на сервер, что позволяет ему сократить временной разрыв между обрабатываемыми и актуальными данными.

База данных NoSQL Apache Cassandra хранит историю событий, на основе которых реконструируется сценарий потенциальной атаки на протяжении длительного временного периода.

Обработка событий в оперативной памяти позволяет существенно повысить скорость прототипа путем избегания взаимодействия с файловой системой, однако прототипу требуется высокая пропускная способность интернета и большой объем оперативной памяти.

В докладе рассматриваются различные методы обработки больших данных, которые применяются для обнаружения многошаговых атак. Анализируются как классические подходы, так и вспомогательные, используемые в комбинации с основными. Представляется текущая реализация прототипа системы обнаружения многошаговых кибератак на основе технологий больших данных, и демонстрируются эксперименты с данным прототипом. В качестве будущих исследований планируется дальнейшее развитие прототипа и проведение экспериментов с ним.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В., Саенко И. Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник Российской академии наук. 2014. Т. 84. № 11. С. 993-1001.
2. Котенко И. В., Ушаков И. А. Технологии больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд, 2017. № 3 С.23-33.
3. Котенко И. В., Федорченко А. В., Саенко И. Б., Кушнеревич А. Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // Вопросы кибербезопасности. 2017. № 5 (23). С.2-16. DOI: 10.21681/2311-3456-2017-5-2-16.
4. Lee S., Huh J. H. An effective security measures for nuclear power plant using big data analysis approach // The Journal of Supercomputing. 2019. Т. 75. С. 4267-4294.
5. Tang M., Alazab M., Luo Y. Big Data for Cybersecurity: Vulnerability Disclosure Trends and Dependencies // IEEE Transactions on Big Data. 2019. Т. 5. № 3. С. 317-329.
6. Kotenko I., Saenko I., Branitskiy A. Machine learning and big data processing for cybersecurity data analysis // Data science in cybersecurity and cyberthreat intelligence. 2020. С. 61-85.
7. Guo Y., Sun Y., Wu K., Jiang K. New Algorithms of Feature Selection and Big Data Assignment for CBR System Integrated by Bayesian Network // ACM Trans. Knowl. Discov., 2020. № 23. 20 с.
8. Moqurrab S. A. Deep-Confidentiality: An IoT-Enabled Privacy-Preserving Framework for Unstructured Big Biomedical Data / S. A. Moqurrab, A. Anjum, A. Khan, A. Mansoor [et al] // ACM Trans. 2021. Т. 22. № 2. 21 с.
9. Vu T., Belussi A., Migliorini S., Eldway A. Using Deep Learning for Big Spatial Data Partitioning // ACM Trans. Spatial Algorithms Syst. 2020. Т. 7. № 1. 37 с.

10. Chen Z., Wang Y., Narasayya V., Chaudhuri S. Customizable and scalable fuzzy join for big data // Proc. VLDB Endow. 2019. Т. 12. № 12. С. 2106–2117.
11. Chen L. Unified Holistic Memory Management Supporting Multiple Big Data Processing Frameworks over Hybrid Memories / L. Chen, J. Zhao, C. Wang, T. Cao, J. Zigman [et al] // ACM Trans. Comput. Syst. 2022. Т. 39. № 1–4. 38 с.
12. Shu J., Fang K., Chen Y., Wang S. TH-iSSD: Design and Implementation of a Generic and Reconfigurable Near-Data Processing Framework // ACM Trans. Embed. Comput. Syst. 2023. 23 с.
13. Song J., He Q., Chen F., Yuan Y., Yu G. PoBery: Possibly-complete Big Data Queries with Probabilistic Data Placement and Scanning // ACM/IMS Trans. Data Sci. 2021. Т. 2. № 3. 28 с.
14. Vinçon T. Near-data processing in database systems on native computational storage under HTAP workloads / T. Vinçon, C. Knödler, L. Solis-Vasquez, A. Bernhardt [et al] // Proc. VLDB Endow. 2022. Т. 15. № 10.С. 1991–2004.
15. Chen N., Drouhard M., Kocielnik R., Suh J., Aragon C. R. Using Machine Learning to Support Qualitative Coding in Social Science: Shifting the Focus to Ambiguity // ACM Trans. Interact. Intell. Syst. 2018. Т. 8. № 2. 20 с.
16. Akgun I. U. Improving Storage Systems Using Machine Learning / I. U. Akgun, A. S. Aydin, A. Burford, M. McNeill [et al] // ACM Trans. Storage. 2023. Т. 19. № 1. 30 с.

УДК 004.056.53

РОЛЬ СТАТИЧЕСКОГО АНАЛИЗАТОРА КОДА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОГРАММНОГО ПРОДУКТА

Знаменская Дарья Денисовна
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mail: zdasha02@gmail.com

Аннотация. В данных материалах автор рассматривает один из прикладных инструментов информационной безопасности — статический анализатор кода — и роль, которую он играет в разработке программного продукта.

Ключевые слова: информационная безопасность, статический анализатор кода, программное обеспечение, уязвимость, защита данных.

THE ROLE OF A STATIC CODE ANALYZER IN INFORMATION SECURITY OF THE PROGRAM PRODUCT

Znamenskaya Daria
Saint Petersburg State University of Aerospace Instrumentation
67 Bolshaya Morskaya St., St. Petersburg, 190121, Russia
e-mail: zdasha02@gmail.com

Abstract. In these materials the author considers one of the information security application tools, a static code analyzer, and the role it plays in program product development.

Keywords: information security, static code analyzer, software, vulnerability, data protection.

Информационная безопасность — обширная область информационных технологий, задачей которой является обеспечение доступности, конфиденциальности и целостности данных [1]. При создании любого программного продукта особое внимание необходимо уделять именно информационной безопасности: различные уязвимости, отсутствие шифрования, передача данных по незащищенных каналам связи и другие недостатки могут привести к серьезным последствиям, например, нарушению коммерческой тайны или прав пользователей. Также высока вероятность, что слабыми местами системы воспользуются злоумышленники с целью хищения информации или проведения кибератаки, что не редкость в настоящее время.

Отдельные проблемы программного обеспечения возникают на этапе его разработки, а конкретно — уязвимости. Уязвимости — допущенные при написании кода ошибки, благодаря которым можно получить несанкционированный доступ к функциям приложения или хранящимся внутри него данным [2]. Часто очень сложно обнаружить уязвимости вручную, а привлечение ряда специалистов — неэффективно и дорого, поэтому на практике широко используют специальные утилиты, называемые анализаторами кода.

В то время как компилятор обычно обнаруживает только синтаксические ошибки, инструменты статического анализа осуществляют более глубокую проверку кода, анализируя программу без ее реального выполнения [3]. Процесс поиска проблемных участков, как правило, состоит из следующих этапов:

– на вход анализатору подается исходный код проекта или, в отдельных случаях, бинарные файлы;
– на основе кода утилита создает специальную модель для ее дальнейшего анализа;
– производится поиск уязвимостей модели на основе набора диагностических правил из различных методологий;
– полученные результаты сохраняются в удобный пользователю формат (текстовая отчетность, диаграммы и т.д.);
– пользователь изучает отчетность и принимает решение об исправлении обнаруженных слабых местах.

Также инструмент анализирует зависимости проекта, так как недостатки могут содержать и используемые в разработке open-source (англ. — с открытым исходным кодом) библиотеки.

Помимо обнаружения ошибок анализатор позволяет контролировать качество кода и помогает следовать утвержденным стандартам разработки программного продукта.

Таким образом, статический анализатор кода — незаменимый инструмент в обеспечении информационной безопасности программного обеспечения, благодаря которому можно быстро выявлять уязвимости и критические ошибки и следить за качеством как собственных, так и сторонних модулей.

СПИСОК ЛИТЕРАТУРЫ

1. Грошева Е. К., Невмержицкий П. И. Информационная безопасность: современные реалии // Бизнес-образование в экономике знаний. 2017. № 3. С. 35-38.
2. Горошко Л. Обзор сканеров кода: взгляд интегратора // Anti-Malware : [сайт]. [2018]. [Электронный ресурс] URL: https://www.anti-malware.ru/analytics/Market_Analysis/code-scanner-view-integrator (дата обращения: 23.06.2023).
3. Крушмнамова Ю. Статический анализ в разработке встраиваемых систем // Tproger : [сайт]. [2021]. [Электронный ресурс] URL: https://tproger.ru/articles/staticheskij-analiz-v-razrabotke-vstraivaemyh-sistem/ (дата посещения: 24.06.2023).

УДК 004.942

О РАЗРАБОТКЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ

Иванцов Дмитрий Сергеевич, Саенко Игорь Борисович
СПИИРАН – СПб ФИЦ РАН,
14-я линия В.О., д. 39, Санкт-Петербург, 199178, Россия
e-mails: dima_ivantsov91@mail.ru, ibsaen@mail.ru

Аннотация. Обсуждается подход к разработке математической модели процесса функционирования системы управления информацией и событиями безопасности, известной как SIEM-система. Данная модель представляет собой формализованное аналитическое описание (в терминах марковской цепи в форме разностных стохастических уравнений) динамики смены состояний показателей качества, характеризующих существенные свойства процесса функционирования системы управления информацией и событиями безопасности, в пространстве состояний. Модель представляет собой традиционную для цепи Маркова, в форме конечных разностей, систему уравнений состояния и наблюдения.

Ключевые слова: математическое ожидание, система управления информацией и событиями безопасности, показатель качества, процесс функционирования, матрица, состояние.

ON THE DEVELOPMENT OF A MATHEMATICAL MODEL OF THE PROCESS OF OPERATION OF THE INFORMATION AND SECURITY EVENT MANAGEMENT SYSTEM

Dmitry Ivantsov, Igor Saenko
SPIIRAS – SPCRAS
39 14th Line St, Petersburg, 199178, Russia
e-mails: dima_ivantsov91@mail.ru, ibsaen@mail.ru

Abstract. An approach to the development of a mathematical model of the process of functioning of the security information and event management system, popularly known as the SIEM system, is discussed. This model represents the formalized analytical description (in terms of the Markov chain in the form of difference stochastic equations) of the dynamics of change of states of quality indicators, characterizing essential properties of the information and security events management system functioning process, in the space of states. The model represents traditional for Markov chain, in the form of finite differences, the system of equations of state and monitoring.

Keywords: mathematical expectation, system of security information and event management, quality indicator, functioning process, matrix, state.

Предлагаемая модель представляет собой инструмент для анализа и оптимизации работы SIEM-системы. Модель базируется на следующих предположениях: (1) SIEM-система имеет конечное количество состояний, которые изменяются со временем; (2) переходы между состояниями происходят с некоторыми вероятностями, которые могут зависеть от текущего состояния и других переменных; (3) каждое состояние характеризуется набором показателей качества, которые можно измерить; (4) измерения показателей качества могут быть зашумлены или недоступны в определенные моменты времени. Модель состоит из системы уравнений состояния и системы уравнений наблюдения. Система уравнений состояния описывает изменение вероятности нахождения системы в каждом из состояний в следующий момент времени. Эта вероятность зависит от текущего состояния и вероятностей перехода между состояниями [1].

Для достижения цели защиты информации, разработка математической модели процесса функционирования SIEM-системы является важным шагом. Такая модель позволяет анализировать и оптимизировать работу SIEM-системы, которая играет ключевую роль в обеспечении безопасности компьютерных и телекоммуникационных сетей.

SIEM-система интегрирует данные о событиях безопасности и информации о состоянии системы, анализирует их и предоставляет оператору информацию о возможных угрозах и инцидентах безопасности.

Однако для эффективной работы SIEM-системы необходимо оптимально настроить ее параметры и конфигурацию.

Математическая модель, предлагаемая в данном случае, основывается на концепции марковской цепи. Марковская цепь — это математическая модель, в которой переход между состояниями системы зависит только от текущего состояния и не зависит от предыдущих состояний. Модель основана на системе уравнений состояния и уравнений наблюдения, которые описывают изменение состояний системы и изменение вероятности получения определенных измерений показателей качества [2].

Модель позволяет анализировать вероятности нахождения системы в разных состояниях и вероятности получения определенных измерений показателей качества. Используя данную модель, можно определить оптимальные параметры SIEM-системы, которые позволят максимизировать эффективность работы системы и минимизировать потери информации.

Модель позволяет проводить анализ и оптимизацию работы системы, что в свою очередь помогает минимизировать потери информации, связанные с доступностью, целостностью и конфиденциальностью данных [3].

SIEM-системы играют важную роль в обеспечении безопасности информации путем анализа событий и угроз в реальном времени. Они представляют собой интегрированные решения, которые объединяют данные о безопасности из различных источников, таких как сетевые устройства и приложения, и осуществляют мониторинг, сбор и анализ этих данных [2].

SIEM-системы также предоставляют функциональность для управления инцидентами безопасности. Они позволяют создавать и отслеживать инциденты, принимать меры для их устранения и анализировать причины и последствия инцидентов.

Применение модели SIEM-системы поможет повысить эффективность ее работы, улучшить способность обнаруживать и реагировать на угрозы информационной безопасности быстро и точно.

Практическая значимость таких исследований состоит в возможности применения модели SIEM-системы в организациях для повышения уровня безопасности и защиты информации. Благодаря детальному аналитическому описанию работы SIEM-системы, организации смогут получить лучшее представление о своей информационной безопасности и обнаруживать потенциальные угрозы раньше.

Кроме того, актуальность и практическая значимость исследований в рамках данной работы связаны с необходимостью постоянного совершенствования SIEM-системы [4]. С постоянным развитием технологий и появлением новых угроз информационной безопасности модель SIEM-системы должна быть обновлена и адаптирована для анализа новых видов атак и защиты от них.

Таким образом, исследования в данной теме являются актуальными и практически значимыми, так как помогают повысить эффективность и надежность функционирования SIEM-систем, которые обеспечивают контроль и защиту информационной безопасности в современных компьютерных сетях.

Традиционным подходом к аналитическому описанию процессов функционирования сложных систем, например, таких, как SIEM-система, являются попытки формально представить данные процессы через динамику линейного или нелинейного изменения состояния (пошаговых значений) показателей качества (ПК) SIEM-системы и процесса ее функционирования в пространстве состояний. Марковские модели процессов в этом случае являются незаменимым инструментом [2].

Под показателями качества SIEM-системы понимается количественная характеристика одного или нескольких свойств этой системы, обуславливающих ее качество. Эта количественная характеристика может иметь векторный вид (вектор ПК). Компоненты вектора ПК представляют собой численные значения одного или нескольких параметров, описывающих конкретное свойство SIEM-системы, а также процессов функционирования различных ее элементов или системы в целом. При этом ПК как количественная характеристика одного или нескольких свойств системы, обуславливающих ее качество, рассматривается применительно к определенным условиям создания SIEM-системы и условиям реализации процесса ее функционирования [5].

Состояние ПК — понятие, обозначающее множество устойчивых значений этого показателя. Их может быть несколько либо большое множество. Состояние ПК характеризуется тем, что описывает переменные свойства этого показателя. При этом состояние какого-либо показателя качества процесса устойчиво до тех пор, пока процесс не реализуется, ведь сам процесс — это последовательная смена состояний показателей, его описывающих.

Использование языка теории множеств и функциональных пространств позволит упростить и структурировать математическое описание процесса функционирования SIEM-системы. Это поможет исследователям лучше понять и представить связи между различными параметрами и состояниями системы [6].

Построение аналитической и вероятностно-временной модели смены состояний ПК на основе марковских последовательностей будет полезно для анализа и прогнозирования вероятности возникновения определенных состояний ПК в различных временных интервалах. Это может помочь оптимизировать работу SIEM-системы и принимать предупредительные меры перед возможными инцидентами информационной безопасности.

Можно сделать вывод о том, что модель может быть полезна для исследования и анализа информационной безопасности. Она может быть использована для определения уязвимостей и потенциальных угроз, а также для оценки эффективности мер безопасности. Для более точного и всестороннего анализа, можно разрабатывать модель, которая учитывает не только количественные показатели качества, но и качественные аспекты. Например, включение лингвистических переменных, типичных для нечетких множеств, может позволить учесть

различные уровни риска или степень угрозы. Это поможет более точно оценивать и классифицировать безопасность информационной системы.

СПИСОК ЛИТЕРАТУРЫ

1. Aytakin N. I. The definitions of information and security; history of information security development // Vilnius University Open Series, 2020. Vol. 6. Pp. 48–57. DOI: 10.15388/OS.LAW.2020.5.
2. Котенко И. В., Паращук И. Б. Модель системы управления информацией и событиями безопасности // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2020. № 2. С. 84–94. DOI: 10.24143/2072-9502-2020-2-84-94.
3. Саенко И. Б., Иванцов Д. С., Ермаков А. В. Модель оценки устойчивости хранения больших данных в распределенной файловой системе // Труды НИИР. 2022. № 4. С. 42–45. DOI: 10.34832/NIIR.2022.11.4.005.
4. Kotenko I. V., Parashchuk I. B. An approach to modeling the decision support process of the security event and incident management based on Markov chains // IFAC-PapersOnLine, 2019. Vol. 52. № 13. Pp. 934–939. DOI: 10.1016/j.ifacol.2019.11.314.
5. Shaikh E., Mohiuddin I., Alufaisan Y., Nahvi I. Apache Spark: A Big Data Processing Engine // 2019 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM), Manama, Bahrain, 2019. Pp. 1-6. DOI: 10.1109/MENACOMM46666.2019.8988541.
6. González-Granadillo G., González-Zarzosa S., Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures // Sensors, 2021. Vol. 21. № 14. P. 4759. DOI: 10.3390/s21144759.

УДК 004.056

МОДЕЛИ АТАК НА КОМПОНЕНТЫ МАШИННОГО ОБУЧЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

Ичетовкин Егор Андреевич, Котенко Игорь Витальевич
СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: ichetovkin.e@iias.spb.su, ivkote@comsec.spb.ru

Аннотация. В настоящее время актуальной задачей является разработка моделей атак на компоненты машинного обучения, которые могут эффективно использоваться для защиты систем обнаружения вторжений критических инфраструктур. В работе рассмотрены модели атак на компоненты машинного обучения систем обнаружения вторжений критических инфраструктур.

Ключевые слова: информационная безопасность; машинное обучение; система обнаружения вторжений; атаки на системы искусственного интеллекта.

MODELS OF ATTACKS ON MACHINE LEARNING COMPONENTS OF INTRUSION DETECTION SYSTEMS FOR CRITICAL INFRASTRUCTURES

Ichetovkin Egor, Kotenko Igor
SPIIRAS – SPCRAS
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: ichetovkin.e@iias.spb.su, ivkote@comsec.spb.ru

Abstract. Currently, an urgent task is to develop attack models for machine learning components that can be effectively used to protect intrusion detection systems of critical infrastructures. The paper considers models of attacks on machine learning components of intrusion detection systems of critical infrastructures.

Keywords: Information security; machine learning; intrusion detection system; attacks on artificial intelligence systems.

В современном мире кибератаки на критические инфраструктуры становятся все более распространенными и опасными [1-3]. Системы обнаружения вторжений (СОВ) являются важным инструментом для защиты таких инфраструктур [1, 4]. С появлением новых угроз и развитием технологий, системы обнаружения вторжений стали использовать компоненты обнаружения, основанные на методах машинного обучения, актуальной стала задача использования моделей атак, для повышения защищенности компонентов машинного обучения систем обнаружения вторжений [5-7].

В работе рассмотрены различные классы моделей атак на компоненты машинного обучения СОВ. Представленные модели атак на компоненты машинного обучения являются аддитивными состязательными атаками, нарушающими работу классификатора [5, 6].

Модель атаки минимизирующей функцию расстояния, основана на изменение входных данных с целью уменьшения значения функции расстояния между исходными данными и целевыми данными. Примером атак этого класса, является атака FGSM (Fast Gradient Sign Method), которая использует градиент функции потерь по отношению к входным данным для создания адверсариальных примеров, уменьшения функции расстояния [7, 8].

Модель атаки, максимизирующей функцию расстояния, основана на изменения входных данных с целью увеличения расстояния между исходными данными и целевыми данными или классом [7, 8].

Модель атаки на основе регуляризации, включает в себя оптимизацию функции потерь с добавлением регуляризационного слагаемого. Регуляризационное слагаемое добавляется для управления изменением исходных данных таким образом, чтобы они были классифицированы неправильно [9, 10].

В работе представлены модели атак на компоненты машинного обучения систем обнаружения вторжений критической инфраструктуры, дано их математическое описание и классификация. Направление дальнейшего

исследования авторы видят в разработке моделей и алгоритмов защиты систем обнаружения вторжений критических инфраструктур от атак на компоненты машинного обучения.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В., Саенко И. Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник Российской академии наук. 2014. Т. 84. № 11. С. 993-1001.
2. Kotenko I., Chechulin A. Computer Attack Modeling and Security Evaluation based on Attack Graphs // Proceedings of the IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS 2013. 2013. С. 614-619.
3. Kotenko I. Agent-Based Modeling and Simulation of Cyber-Warfare between Malefactors and Security Agents in Internet // 19th European Simulation Multiconference «Simulation in wider Europe». Riga, Latvia, 1–4 June 2005. ECMS 2005. P.533-543.
4. Bhattacharya P., Kalita J. Deep learning and its applications in intrusion detection systems // Journal of Information Security and Applications. 2017. P. 40-48.
5. Huang L., Joseph A. D., Nelson B., Rubinstein B. I., Tygar J. D. Adversarial machine learning // Proceedings of the 4th ACM workshop on Security and artificial intelligence. 2007. P. 43-58.
6. Papernot N., McDaniel P., Sinha A., Wellman M. SoK: Security and privacy in machine learning // Proceedings of the IEEE Symposium on Security and Privacy. 2018. P. 399-414.
7. Rieck K., Holz T., Willems C., Düssel P., Laskov P. Learning and classification of malware behavior // Journal of Machine Learning Research, 9(Oct). 2008. P. 2721-2764.
8. Shafiq M. Z., Khan S., Khayam S. A. Towards generating realistic anomalies for network intrusion detection // Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining. 2009. P. 1247-1256.
9. Xu W., Evans D., Qi Y. Feature squeezing: Detecting adversarial examples in deep neural networks // Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 2017. P. 1395-1404.
10. Zhu S., Zou C., Li J. Adversarial examples for malware detection // IEEE Transactions on Dependable and Secure Computing, 2019. 16(1). P.24-37.

УДК 004.056.5

УРОВНИ АРХИТЕКТУРЫ КОМПОНЕНТОВ ОПЕРАТИВНОЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ РЕСУРСОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Котенко Игорь Витальевич, Саенко Игорь Борисович, Паращук Игорь Борисович
СПИИРАН – СПб ФИЦ РАН
14-я линия ВО, 39, Санкт-Петербург, 194064, Россия,
e-mails: ivkote@comsec.spb.ru, ibsaen@comsec.spb.ru, shchuk@rambler.ru

Аннотация. Предложен подход к построению обобщенной архитектуры компонентов оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов на основе аналитической обработки больших массивов гетерогенных данных. Данный подход базируется на функциональных характеристиках модулей основной и вспомогательной группы обобщенной архитектуры данных компонентов. Рассматриваемая архитектура позволяет своевременно оценивать и идентифицировать угрозы для информационных и телекоммуникационных ресурсов критической инфраструктуры, их возможные источники, определять вероятности возникновения коллизий, а также оценивать их последствия для всех возможных вариантов развития ситуации.

Ключевые слова: компоненты, архитектура, оперативная оценка защищенности, группа, уровень, модули, ресурсы, аналитическая обработка, большие массивы гетерогенных данных.

LEVELS OF ARCHITECTURE OF COMPONENTS OF OPERATIONAL ASSESSMENT OF SECURITY OF INFORMATION AND TELECOMMUNICATION RESOURCES OF CRITICAL INFRASTRUCTURE

Kotenko Igor, Saenko Igor, Parashchuk Igor
SPIIRAS – SPCRAS
39, 14-th Linia, VI, St. Petersburg, 199178, Russia
e-mails: ivkote@comsec.spb.ru, ibsaen@comsec.spb.ru, shchuk@rambler.ru

Abstract. An approach to the construction of a generalized architecture of components for the operational assessment of the security of information, telecommunications and other critical resources based on the analytical processing of large arrays of heterogeneous data is proposed. This approach is based on the functional characteristics of the modules of the main and auxiliary groups of the generalized architecture of these components. The architecture under consideration allows timely assessment and identification of threats to information and telecommunication resources of critical infrastructure, their possible sources, to determine the likelihood of collisions, as well as to assess their consequences for all possible scenarios of the situation.

Keywords: components, architecture, operational security assessment, group, level, modules, resources, analytical processing, large arrays of heterogeneous data.

Разработка архитектуры и программных прототипов компонентов оперативной оценки защищенности (ООЗ) информационных, телекоммуникационных ресурсов (ИТР) и других критически важных ресурсов (КВР) на основе аналитической обработки (АО) больших массивов гетерогенных данных (БМГД) может и должна быть реализована с целью проверки работоспособности моделей и алгоритмов такой оценки. Важность защиты ИТР и других КВР обуславливает актуальность множества современных исследований в данной области [1-3].

Понимая под архитектурой принципиальную организацию компонентов системы, воплощенную в их конкретных уровнях и элементах, их взаимоотношениях друг с другом и со средой, а также принципы, направляющие их проектирование и эволюцию, сформулируем сущность и функционал уровней (граней) архитектуры компонентов ООЗ ИТР и других КВР на основе АО БМГД.

Общая архитектура компонентов ООЗ ИТР и других КВР на основе АО БМГД включает два компонента (уровня): компонент высокого уровня, который, помимо прочего, обеспечивает взаимосвязь этого компонента, например, со средствами суперкомпьютера и компонент низкого уровня. Исходными данными является структура информационных потоков, циркулирующих между компонентами системы АО БМГД о событиях кибербезопасности в интересах оценки состояния, поддержки принятия решений и расследования компьютерных инцидентов в критически важных инфраструктурах, а также обобщенные алгоритмы функционирования такой системы в различных режимах и с учетом особенностей современных технологий, вычислительной техники, сетей и телекоммуникаций [4, 5].

Комплексная методика ООЗ на основе АО БМГД включает четыре стадии: стадию сбора исходных данных; стадию построения моделей и методов (моделей и методов оценки вероятности и воздействия путей риска на защищенность ИТР и других КВР, моделей и методов оценки сетевых (ресурсных) рисков защищенности ИТР и других КВР, моделей и методов оценки выбора пути высокого риска защищенности ИТР и других КВР); стадию разработки и реализации алгоритмов ООЗ ресурсов с использованием возможностей суперкомпьютера (алгоритмов построения сетевой модели, алгоритмов построения графа риска, алгоритмов выделения путей риска, алгоритмов оценки вероятности и воздействия путей риска, алгоритмов оценки сетевых рисков и алгоритмов выбора пути высокого риска) и стадию реализации методики ООЗ ресурсов (включая взаимодействие между компонентами).

С учетом этих стадий рассмотрим архитектуру компонентов ООЗ ИТР и других КВР на основе АО БМГД через функциональные характеристики модулей (элементов, подсистем) основной и вспомогательной группы общей архитектуры данных компонентов. Архитектура компонентов ООЗ ИТР и других КВР на основе АО БМГД включает два уровня: высокий и низкий. При этом архитектура компонента высокого уровня содержит функциональные модули основной группы и, помимо решаемых ими задач, отвечает за взаимосвязь этого компонента со средствами суперкомпьютера, а архитектура компонента низкого уровня содержит функциональные модули вспомогательной группы. При этом формализация и непосредственная работа с информационными потоками в интересах АО БМГД предполагается на всех уровнях архитектуры компонентов ООЗ ИТР и других КВР, например, с применением методов интервального анализа защищенности [6, 7].

Таким образом, архитектура компонентов ООЗ ИТР и других КВР на основе АО БМГД включает две группы модулей (элементов, подсистем): основная группа модулей (элементов, подсистем) включает: модуль построения модели сети, модуль формирования путей риска, модуль оценки рисков и модуль выбора пути высокого риска; вспомогательная группа модулей (элементов, подсистем) включает: модуль сбора и предварительной обработки исходных данных, модуль ведения рабочей базы данных (репозиторий), модуль взаимодействия с другими компонентами и модуль взаимодействия с пользователями.

Иными словами, в основную группу, составляющую компонент высокого уровня, будут входить модули, непосредственно выполняющие ООЗ ИТР и других КВР с использованием возможностей суперкомпьютера.

Рассмотрим функциональные задачи, решаемые конкретными модулями, входящими в основную группу, составляющую компонент высокого уровня в рамках общей архитектуры компонентов ООЗ ИТР и других КВР на основе АО БМГД. В модуле построения модели сети производится преобразование топологии сети, представленной в некотором формате, который будет задаваться параметрами конфигурации компонента, в модель сети. Для реализации этого преобразования используются данные, содержащиеся в рабочей базе данных компонента. Модуль формирования путей риска компонента высокого уровня предназначен для реализации алгоритмов построения графа риска и алгоритмов выделения путей риска. В качестве исходных данных он использует результат первого модуля — модуля построения модели сети. Модуль оценки рисков компонента высокого уровня предназначен для реализации алгоритмов оценки вероятности и воздействия путей риска и алгоритмов оценки сетевых рисков. Входными данными для этого модуля являются результаты работы первого и второго основных модулей. Четвертый основной модуль компонента высокого уровня предназначен для реализации алгоритмов выбора пути высокого риска.

Рассмотрим функциональные задачи, решаемые конкретными модулями, входящими во вспомогательную группу, составляющую компонент низкого уровня в рамках общей архитектуры компонентов ООЗ ИТР и других КВР на основе АО БМГД.

Модули вспомогательной группы реализуют функции, обеспечивающие сбор и хранение исходных данных и промежуточных результатов, а также взаимодействие с другими компонентами и пользователями.

Таким образом, уровень архитектуры компонента низкого уровня (вспомогательная группа), характеризующий функциональные задачи данного компонента, представлены модулями (подсистемами) сбора и предварительной обработки исходных данных, ведения рабочей базы данных (репозитория), взаимодействия с другими компонентами и взаимодействия с пользователями.

Второй уровень (грань) архитектуры компонента низкого уровня (вспомогательная группа), отвечающий за конкретные предметные области ООЗ — объекты оценки защищенности, содержит:

критические информационные ресурсы, критические телекоммуникационные ресурсы и другие критически важные ресурсы, оцениваемые с помощью АО БМГД. На уровне сервисов обработки данных архитектуры компонента низкого уровня (вспомогательная группа) осуществляется сбор данных об оценочных значениях показателей защищенности ресурсов, их обобщение, нормализация и предварительная корреляция. С учетом рассмотренных и исследованных особенностей архитектуры, программные прототипы компонентов ООЗ основаны на использовании открытых библиотек и способны обеспечивать взаимодействие с другими прототипами целевой системы. Кроме того, они учитывают особенности выполнения программ в среде суперкомпьютера, свойственные параллельно-массивной обработке данных и решению масштабных задач в условиях кластерной архитектуры суперкомпьютерной системы, в которой используется технология Message Passing Interface и графические ускорители.

Работа выполнена при финансовой поддержке гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Блюмин А. М., Феоктистов Н. А. Мировые информационные ресурсы : учеб. пособие. М. : Издательско-торговая корпорация «Дашков и К°», 2010. 296 с.
2. Setola R., Luiijf E., Theoharidou M. Critical Infrastructures, Protection and Resilience // Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control. Springer, 2016. Pp. 1-18.
3. Basch E. M., Thaler H. T., Shi W., Yakren S., Schrag D. Use of information resources by patients with cancer and their companions // Cancer: Interdisciplinary International Journal of the American Cancer Society. № 100(11), 2004. Pp. 2476-2483.
4. Гребешков А. Ю. Вычислительная техника, сети и телекоммуникации : учеб. пособие для вузов. М. : ГЛТ, 2016. 190 с.
5. Bouras C. J. Trends in Telecommunications Technologies. Patras: (Greece), InTech, 2010. 778 p.
6. Котенко И. В., Паращук И. Б. Интервальный анализ защищенности телекоммуникационных ресурсов критически важных инфраструктур // Математические методы в технологиях и технике : сборник трудов Международной научной конференции ММТТ-35. № 1, 2022. СПб. : Издательство Политехнического университета. 2022. Т. 1. С. 64-67.
7. Котенко И. В., Паращук И. Б. Информационные и телекоммуникационные ресурсы критически важных инфраструктур: особенности интервального анализа защищенности // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2022. № 2. С. 33-40.

УДК 004.9

АВТОМАТИЗАЦИЯ ПРОЦЕССА ПОДГОТОВКИ МАТЕРИАЛОВ В РАМКАХ ПРОЕКТА «ПУШКИН ЦИФРОВОЙ»

Котов Александр Александрович, Кокорин Павел Петрович
СПИИРАН – СПб ФИЦ РАН
14 линия, 39, Санкт-Петербург, 199178, Россия
e-mail: alexanderkotovspb@gmail.com

Аннотация. Рассматривается подход к автоматическому формированию полного библиографического описания всех материалов, входящих в литературное наследие А. С. Пушкина в едином унифицированном формате для последующего использования в рамках проекта «Пушкин Цифровой».

Ключевые слова: обработка естественного языка; образовательный портал; наследие Пушкина.

AUTOMATION OF THE PROCESS OF PREPARATION OF MATERIALS WITHIN THE FRAMEWORK OF THE PUSHKIN DIGITAL PROJECT

Kotov Alexander, Kokorin Pavel
SPIIRAS – SPCRAS
39 14th Line St, Petersburg, 199178, Russia
e-mails: alexanderkotovspb@gmail.com

Abstract. An approach to the automatic generation of a complete bibliographic description of all materials included in the literary heritage of A.S. Pushkin in a single unified format for subsequent use within the framework of the «Pushkin Digital» project is considered.

Keywords: natural language processing; educational portal; literary heritage of Pushkin.

В эпоху информационных технологий и бурного развития искусственного интеллекта гуманитарные науки сталкиваются с уникальными возможностями и вызовами в контексте анализа и обработки больших массивов информации. В центре нашего исследования — тома произведений выдающегося русского поэта и писателя А. С. Пушкина, включая материалы с его личными комментариями и заметками. Обработка оцифрованных документов является первостепенной задачей в контексте сохранения и цифровой реставрации литературных произведений. Оцифрованный формат не только предоставляет удобный доступ к источникам, но и позволяет применять разнообразные алгоритмы обработки и анализа текста.

Современное научное и технологическое пространство включает в себя сложные методы обработки информации, которые могут быть основаны на принципах машинного обучения, глубокого анализа данных и семантической обработки текста. В этой связи целью исследования является создание комплексной системы для эффективного извлечения и представления информации из текстов произведений А. С. Пушкина, которая в дальнейшем обрабатываются методами обработки естественного языка (NLP), машинного и глубокого

обучения [1]. В текущий момент создание такого ресурса является стратегическим и социально значимым проектом в области культуры [2].

Несмотря на то, что некоторые подходы к автоматизации разработки образовательных ресурсов предлагались авторами ранее [3], часть технологий, используемых в проекте являются технологиями общего назначения (NLP-библиотеки, статистический анализ, web-технологии) все равно остаются не решенные научные и технологические задачи.

В частности, потребовалось разработать алгоритмический аппарат и его программную реализацию, которая однозначно раскроет сокращения из текста энциклопедической статьи для создания полного библиографического описания. При этом необходимо минимизировать перечень сокращений, которые не удается раскрыть и сформировать из них отдельный список для ручной обработки.

Примерами таких записей могут быть: «фотокопия ПД, ф. 244, оп. 1. Прилож. № 10 (беловой; был в альбоме С. Н. Карамзиной). ПД 24 (беловой, первой редакции, под заглавием «Вольность. Ода»); ПД 33 (ст. 75–96; беловой, поздней редакции); РГАЛИ, ф. 195, оп. 1, № 5549, л. 4–4 об. (ст. 1–40; поздней редакции, под заглавием «Свобода»; копия рукой неустановленного лица, с поправкой Пушкина); ПД 875 (ст. 41–96; поздней редакции, копия рукой неустановленного лица, с поправками Пушкина) и др.

Для решения задачи разработан алгоритм, включающий чтение данных из файла docx, поиска абзаца с началом списка указателя имен, парсинг строки при помощи механизма регулярных выражений, нормализацию строки (в частности, удаления пробелов и иных символов форматирования в конце и начале строк), сохранения результатов в базу данных с формированием универсального идентификатора.

Идентификация всех обработанных рукописей формируется по единому правилу:

– ПД — Постоянный префикс, встречается практически во всех документах Пушкинского дома.
– 845 — Порядковый номер описи (отдельный лист, тетрадь, книга), может содержать от 1 до 4 цифр.
– л. 15, 49–48 об., 47 об. — 46 об. — Листы (нумеруются ТОЛЬКО листы, при этом 49 — это лицевая сторона листа, 48 об. — оборотная сторона листа).

Программная реализация оформлена в виде функции на языке python и включена в состав программных средств по проекту «Пушкин Цифровой».

СПИСОК ЛИТЕРАТУРЫ

1. Pushkin Digital — проект цифрового академического издания сочинений А. С. Пушкина [Электронный ресурс]. URL: https://www.pushkin-digital.ru/ (дата обращения: 30.09.2023).
2. В России запустят портал «Пушкин Цифровой» с рукописями и черновиками [Электронный ресурс]. URL: https://www.interfax.ru/culture/905098 (дата обращения: 30.09.2023).
3. О создании инфологических систем поддержки процесса «обучения через развлечение» (edutainment) / П. П. Кокорин [и др.] // Информационно- измерительные и управляющие системы, 2009. №11. Т. 7. С.42-48.

УДК 004.056

СПОСОБЫ АУТЕНТИФИКАЦИИ И ИХ РОЛЬ В ЗАЩИТЕ ИНФОРМАЦИИ

Крестьяшин Никита Антонович [1], Пучков Владимир Викторович [2]
[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
[2] СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: kaktuz28@mail.ru, puchkov-81@bk.ru

Аннотация. В работе рассмотрены несколько основных видов аутентификации, их преимущества, недостатки, а также статистические данные об их использовании.

Ключевые слова: аутентификация, методы, виды, пароль, смарт-карта, биометрия.

AUTHENTICATION METHODS AND THEIR ROLE IN INFORMATION PROTECTION

Krestyashin Nikita [1], Puchkov Vladimir [2]
[1] St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich
22 Bolshevikov Av., 1, St. Petersburg, 193232, Russia
[2] SPIIRAS – SPCRAS
39 14th Line St., St. Petersburg, 199178, Russia
e-mail: kaktuz28@mail.ru, puchkov-81@bk.ru

Abstract. The paper considers several main types of authentication, their advantages, disadvantages, as well as statistical data on their use.

Keywords: authentication, methods, types, password, smart card, biometrics.

В современном цифровом мире безопасность является одним из главных приоритетов. В основе обеспечения безопасности информации лежит аутентификация — процесс проверки подлинности пользователя или устройства. В данном исследовании рассмотрены несколько основных видов аутентификации, их преимущества, недостатки, а также статистические данные об их использовании.

Аутентификация является фундаментальным аспектом безопасности в информационных системах. В ее основе лежит идея проверки и подтверждения подлинности субъектов, устройств или сервисов, что обеспечивает контроль доступа к конфиденциальной информации [1,2]. В процессе аутентификации проверяется информация, предоставленная пользователем, она сверяется с базой данных и, при наличии совпадения пользователю предоставляется доступ в систему. Большинство систем аутентификации состоит из следующих элементов: субъект, характеристика субъекта, владелец системы аутентификации, механизм аутентификации, механизм авторизации.

В процессе развития технологий и выявления новых угроз безопасности, появляются и совершенствуются новые методы аутентификации. Классификация [3,4] видов аутентификации позволяет подробно рассмотреть каждый способ, обозначить плюсы и минусы всех подходов, а также выбрать наиболее подходящие в зависимости от ресурса, к которому необходимо получить доступ, требований к безопасности, финансовых возможностей и удобства для субъекта.

По характеристике субъекта аутентификацию можно разделить на 3 большие группы: то, что знает субъект; то, чем владеет субъект; то, чем является субъект.

Различные виды аутентификации, будь то пароль, смарт-карта или биометрические данные, являются важным процессом в любой информационной системе [5, 6]. Биометрия — это наиболее защищенная система аутентификации, которой отдают предпочтение производители мобильных устройств, однако у данного подхода также есть некоторые недостатки, которые необходимо устранить в будущем. Следовательно, использование нескольких биометрических данных или комбинации методов аутентификации может помочь обеспечить более высокую безопасность данных.

СПИСОК ЛИТЕРАТУРЫ

1. Заярная И. А., Петрич А. Р. Аутентификация: теоретические аспекты // Вестник Алтайской академии экономики и права. 2022. № 10-3. С. 416-420.
2. Дьяченко Н. В., Отакулов А. С., Шатомиров И. С. Понятие аутентификации, ее применение и особенности // Modern Science. 2019. № 5-3. С. 240-242.
3. Ганижева Н. Ж. Аутентификация и ее виды // Междисциплинарность научных исследований как фактор инновационного развития. 2022. С. 35-36.
4. Усубакунова Г. М., Шаршеева К. Т. Обзор и анализ методов аутентификации пользователей в системах тестирования // Известия Кыргызского государственного технического университета им. И. Раззакова. 2021. № 1. С. 129-136.
5. Михайлова А. А., Мороз А. Р., Уманский С. А., Шустрова А. Н. Двухфакторная аутентификация // Инновационные аспекты развития науки и техники. 2021. № 7. С. 45-50.
6. Десницкий В. А., Сахаров Д. В., Чечулин А. А., Ушаков И. А., Захарова Т. Е. Защита информации в центрах обработки данных : учеб. пособие. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2019. 92 с.

УДК 003.26

ОБЗОР АЛГОРИТМОВ ЦИФРОВОЙ ПОДПИСИ СО СКРЫТОЙ ГРУППОЙ

Курышева Алена Андреевна
СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: kurysheva.al@yandex.ru

Аннотация. Рассматриваются различные варианты алгоритмов цифровой подписи со скрытой группой, особенности их реализации. Данные алгоритмы обладают высокой производительностью и актуальны для дальнейших исследований в связи с достигнутыми успехами в области квантовых вычислений.

Ключевые слова: информационная безопасность; криптография; цифровая подпись.

OVERVIEW OF DIGITAL SIGNATURE ALGORITHMS WITH A HIDDEN GROUP

Kurysheva Alena
SPIIRAS – SPCRAS
39 14-th Linia, VI, St. Petersburg, 199178, Russia
e-mails: kurysheva.al@yandex.ru

Abstract. Various variants of digital signature algorithms with a hidden group are considered, the features of their implementation. These algorithms have high performance and are relevant for further research in connection with the successes achieved in the field of quantum computing.

Keywords: information security; cryptography; digital signature.

Учитывая успехи в области квантовых вычислений, становится актуальным проведение исследований по поиску постквантовых шифров и алгоритмов цифровой подписи различных типов, что подтверждается несколькими конкурсами, проводимыми Национальным институтом стандартов и технологий (НИСТ) США. Алгоритмы цифровой подписи со скрытой группой не рассматривались НИСТ, данные алгоритмы имеют высокую производительность и могут быть кандидатами на постквантовые стандарты [1, 2].

Согласно [4] различают алгоритмы электронной цифровой подписи, стойкость которых основана на вычислительной трудности скрытой задачи дискретного логарифмирования, а также алгоритмы, стойкость которых основана на вычислительной трудности решения системы из многих квадратных уравнений с многими неизвестными.

Можно использовать подход [2, 5], основанный на вычислительной сложности скрытой задачи дискретного логарифмирования (ЗДЛ) и связанный с использованием конечных коммутативных ассоциативных алгебр. Конечные коммутативные ассоциативные алгебры используются в качестве носителя.

В алгоритмах данного типа используется секретная скрытая группа, в которой выполняются операции экспоненцирования (операции задания базовой вычислительно трудной задачи) при формировании открытого ключа и генерации цифровой подписи, которые приводят к заданию скрытой ЗДЛ как базового криптографического примитива. Конечные *m*-мерные алгебры согласно [5] можно задать как конечное *m*-мерное векторное пространство с дополнительно определенной замкнутой операцией умножения всевозможных пар векторов, при этом у операции присутствует свойство дистрибутивности слева и справа относительно операции сложения векторов. Алгебры могут быть заданы по прореженным таблицам умножения базисных векторов над конечными полями *GF(p)* [2, 5].

Для повышения производительности алгебраических алгоритмов со скрытой группой можно также использовать в качестве алгебраического носителя конечные некоммутативные ассоциативные алгебры, заданные по прореженным таблицам умножения базисных векторов [4].

Могут также применяться алгоритмы, основанные на вычислительной трудности решения систем многих квадратичных уравнений с многими переменными. Для решения этой вычислительной задачи квантовый компьютер не эффективен — согласно [3] для схем электронной подписи на некоммутативных алгебрах, являющихся постквантовыми, размер открытого ключа и подписи равен примерно 512 байт и 160 байт соответственно, которые намного меньше размеров схем цифровой подписи, выбранных для стандартизации по результатам 3 тура конкурса НИСТ.

Таким образом, рассмотрены различные алгоритмы цифровой подписи со скрытой группой, данные алгоритмы обладаю высокой производительности, поэтому представляют интерес для дальнейших исследований.

СПИСОК ЛИТЕРАТУРЫ

1. Теоретический минимум и алгоритмы цифровой подписи : учебное пособие. СПб.: БХВ-Петербург, 2010. 304 с.
2. Молдовян Д. Н., Костина А. А., Курышева А. А. Протокол слепой подписи, основанный на скрытой задаче дискретного логарифмирования в коммутативной алгебре // Вопросы защиты информации. 2021. №1 (132). С. 16-25. [Электронный ресурс]. URL: https://www.elibrary.ru/item.asp?id=44872100 (дата обращения: 20.06.2023).
3. Молдовян Д. Н., Молдовян А. А., Молдовян Н. А. Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах // Вопросы кибербезопасности. 2022. №1 (47). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/novaya-kontseptsiya-razrabotki-postkvantovyh-algoritmov-tsifrovoy-podpisi-na-nekommutativnyh-algebrah (дата обращения: 20.06.2023).
4. Курышева А. А., Костина А. А., Молдовян Н. А. Алгебраические алгоритмы со скрытой группой над конечными полями характеристики два // Вопросы защиты информации. 2022. № 2 (137). С. 13-20. [Электронный ресурс]. URL: https://elibrary.ru/item.asp?edn=jefcmk (дата обращения: 20.06.2023).
5. Молдовян А. А., Костина А. А., Курышева А. А. Протокол слепой подписи с удвоенным проверочным уравнением // Вопросы защиты информации. 2022. №1 (136). С. 23-27. [Электронный ресурс]. URL:https://www.elibrary.ru/item.asp?id=48112198 (дата обращения: 20.06.2023).

УДК 004.056

КОНСТРУИРОВАНИЕ ПРИЗНАКОВ АТАК САМООРГАНИЗУЮЩЕЙСЯ ДЕЦЕНТРАЛИЗОВАННОЙ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

Мелешко Алексей Викторович
СПИИРАН – СПб ФИЦ РАН
14 линия ВО, 39, Санкт-Петербург, 199178, Россия
e-mail: meleshko.a@iias.spb.su

Аннотация. В работе описан процесс разработки признакового пространства для обнаружения атак в беспроводных сенсорных сетях (БСС) с помощью методов машинного обучения. Рассматриваются атаки, направленные на модификацию или прослушивание данных в БСС, такие как Sinkhole, Wormhole, Sybil и другие. В качестве источника данных выступает самоорганизующаяся децентрализованная БСС с ролевым функционированием. Анализ релевантных работ показал, что признаки для обнаружения описаны в общем виде или не учитывают специфику БСС, а именно наличие свойств децентрализации и самоорганизации. Поэтому был сконструирован новый набор признаков, которые включают в себя как признаки, использовавшиеся ранее в других работах, так и признаки, которые добавляются при реализации свойства децентрализации и ролевого функционирования в сети. Изначально были проанализированы данные, которые можно собрать с БСС, а далее, на их основе было построено признаковое пространство для обнаружения атак в самоорганизующейся децентрализованной БСС, в том числе атак на служебные и пользовательские данные.

Ключевые слова: беспроводная сенсорная сеть, самоорганизующаяся сеть, безопасность беспроводных сенсорных сетей, признаковое пространство, набор данных, сбор данных.

CONSTRUCTION OF ATTACK FEATURES FOR A SELF-ORGANIZING DECENTRALIZED WIRELESS SENSOR NETWORK

Meleshko Aleksei
SPIIRAS – SPCRAS
39, 14-th Linia, St. Petersburg, 199178, Russia
e-mail: meleshko.a@iias.spb.su

Abstract. The paper describes the process of developing a feature space for detecting attacks in wireless sensor networks (WSN) using machine learning methods. Attacks aimed at modifying or listening to data in the WSN, such as Sinkhole, Wormhole, Sybil and others, are considered. A self-organizing decentralized WSN with role-based functioning acts as a data source. The analysis of relevant works showed that the signs for detection are described in general terms or do not take into account the specifics of the WSN, namely the presence of decentralization and self-organization properties. Therefore, our own features were constructed, which include both the features that were previously used in other works, and the features that are added when implementing the properties of decentralization and role-based functioning in the network. Initially, the data that can be collected from the WSN was analyzed, and then, on their basis, a feature space was built to detect attacks on service and user data in the WSN.

Keywords: wireless sensor network, self-organizing network, security of wireless sensor networks, features, data set, data collection.

Детектирование атакующих воздействий в беспроводных сенсорных сетях (БСС) является актуальной задачей в настоящее время. Самоорганизующиеся децентрализованные БСС предполагают возможность динамического изменения состава узлов и устройств БСС, выстраивания сетевой топологии и использование различных ролевых моделей узлов функционирования сети, назначаемых и переопределяемых в процессе работы сети. Одним из примеров таких БСС является система антикризисного управления в чрезвычайных ситуациях, которая обеспечивает сетевую связность и коммуникации сети разнородных устройств, относящихся к различным службам спасения. Атакующие воздействия на подобного рода сети могут иметь катастрофические последствия, например, потеря данных от какого-либо участка сети. Поэтому важно своевременно детектировать атаки для минимизации последствий от их реализации. Одним из эффективных способов обнаружения атак является использование методов машинного обучения. Однако, для применения методов машинного обучения необходимо правильно подобрать признаки, которые будут использоваться для обнаружения атак и позволят достичь приемлемого качества детектирования. Данная работа описывает процесс создания признакового пространства для обнаружения атак, которые направлены на модификацию или подслушивание данных в БСС, таких как Sinkhole, Wormhole, Sybil и пр., реализуемых через эксплуатацию свойств самоорганизации и децентрализации БСС. Приводится описание видов данных, собираемых с рассматриваемой БСС, которые необходимы для обнаружения атак, а также описание конкретных признаков, которые будут использоваться в качестве входных данных для методов машинного обучения.

Был проведен поиск и анализ статей в области обнаружения атак в БСС. Например, в работе [1] описывается атака Sinkhole. Атакующий узел убеждает окружающих, что передача данных через него является кротчайшим маршрутом. В итоге узлы передают данные только через атакующий (контролируемый атакующим) узел. Авторы представляют обзор методов по детектированию данной атаки, а именно методы статистического анализа трафика сети и использование нейронных сетей.

В статье [2] описана атака Wormhole, задача которой заключается в перехвате сообщения от одного узла другому и более быстрая его доставка (за меньшее количество ретрансляций), в результате легитимное сообщение будет отброшено узлом получателем. Авторы предлагают протокол централизованной маршрутизации, который позволяет обнаруживать Wormhole-атаки. Сравнивается ожидаемое время доставки данных от источника до получателя и реальное время доставки. В случае наличия атаки реальное время доставки данных будет значительно меньше ожидаемого. Статья [3] посвящена описанию различных атак на БСС, в частности Sybil-атаке. Суть данной атаки в том, что БСС воспринимает один зараженный узел как несколько узлов. Данное явление нарушает правила маршрутизации в сети, что негативно сказывается на работе БСС. Авторами не представлено описание механизмов и признаков для обнаружения Sybil-атаки.

По результатам анализа можно сделать вывод, что часть статей рассматривают базовые реализации атак, которые не учитывают свойство децентрализации и ролевое функционирование сети (а данные свойства порождают новые признаки для обнаружения). Также в некоторых работах (например, в [3]) не приводится описание признаков, которые авторы используют для обнаружения, либо они описаны в общем виде без указания места сбора данных для получения конкретных признаков для обнаружения. Поэтому задача конструирования признакового пространства для обнаружения атак в самоорганизующейся децентрализованной БСС является актуальной.

Для начала были определены виды данных, которые необходимо собирать с узлов самоорганизующейся децентрализованной БСС. Среди данных можно выделить следующие: маршруты сообщений БСС (маршруты по которым передавались сообщения по сети, могут быть получены из таблиц маршрутизации каждого узла); запросы на перераспределение ролей узлов (события инициирования ролевого перераспределения во время работы сети, собирается из служебного лога контроллера сети); размер полезной нагрузки пакетов данных; геолокация узлов (текущее местоположение каждого уза сети, собирается у каждого узла); потребление ресурсов

узлов, (нагрузка процессора, потребление памяти, остаток энергоресурсов); события добавления новых узлов в сеть и ухода узлов из сети (собирается из служебного лога контроллера сети); качество беспроводного сигнала (собирается у каждого узла сети).

Далее, основываясь на релевантных видах, собираемых данных, были сконструированы конкретные признаки для обнаружения атак в самоорганизующихся децентрализованных БСС. Выделяются следующие признаки: количество уникальных маршрутов, проходящих через определенный узел за единицу времени (вычисляется из данных о маршрутах сообщений БСС, необходим для обнаружения атак Sinkhole, Wormhole и Sybil); запросы на смену ролей узлов сети и его атрибуты (включают в себя информацию об инициаторе запроса и его характеристиках, позволяют обнаруживать атаки, реализованные через нелегитимное использование механизм ролевого функционирования); атрибуты события добавления узла в сеть (геолокация добавляющегося узла и его ресурсные характеристики); средняя частота смены ролей узлов сети (вычисляется из данных в запросах на перераспределение ролей); потребление ресурсов узлов за единицу времени (вычисляется из данных о потреблении ресурсов узлов, в случае резкого увеличения потребления ресурсов у конкретного узла может являться признаком реализации атаки в сети); геолокация узлов; количество событий добавления узлов в сеть за единицу времени (рассчитывается исходя из событий добавления узлов в сеть, большое значение данного признака может говорить о наличии атаки в сети); качество беспроводного сигнала.

Анализируя перечисленные ранее признаки, атакующие воздействия на БСС могут быть успешно обнаружены. Например, атака Sinkhole может быть обнаружена, используя признаки «количество уникальных маршрутов, проходящих через определенный узел за единицу времени», «запросы на смену ролей узлов сети и его атрибуты» и «потребление ресурсов узлов за единицу времени». Поскольку атака реализует перенаправление всего трафика в сети через один зараженный узел, то количество маршрутов через него увеличится, а также увеличится потребление его ресурсов, а в случае реализации данной атаки через механизм ролевого функционирования запрос на перераспределение ролей также может свидетельствовать о начале атаки.

Работа описывает основные виды данных, которые необходимо собирать в самоорганизующейся децентрализованной БСС, а также описывает конкретные признаки для обнаружения атак. Полученный набор признаков учитывает специфику рассматриваемой БСС, а также направлен на обнаружение атак, которые могут быть реализованы с эксплуатацией свойств самоорганизации и децентрализации сети. В дальнейшем планируется провести эксперименты по моделированию рассмотренных атак на фрагменте программно-аппаратного стенда БСС и реализовать механизмы их обнаружения с использованием полученных признаков и известных методов машинного обучения.

СПИСОК ЛИТЕРАТУРЫ

1. Rehman, Au., Rehman, S. U. & Raheem, H. Sinkhole Attacks in Wireless Sensor Networks — A Survey / Wireless Personal Communications, 2019. No. 106. pp. 2291–2313. doi:10.1007/s11277-018-6040-7.
2. O. R. Ahutu, H. El-Ocla. Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks / IEEE Access, 2020, vol. 8, pp. 63270-63282, doi: 10.1109/ACCESS.2020.2983438.
3. Grover J., Sharma S. Security Issues in Wireless Sensor Network — A Review / 5th International Conference on Reliability. Infocom Technologies and Optimization (ICRITO). 2016. Pp. 397-404.

УДК 004.056

ПОДХОД К РОЛЕВОМУ ФУНКЦИОНИРОВАНИЮ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

Мелешко Алексей Викторович
СПИИРАН – СПб ФИЦ РАН
14 линия ВО, 39, Санкт-Петербург, 199178, Россия
e-mail: meleshko.a@iias.spb.su

Аннотация. Работа посвящена описанию механизмов ролевого функционирования различных беспроводных сенсорных сетей (БСС). Ролевое управление в БСС направлено на распределение функций базовой станции на несколько узлов сети, что положительно сказывается на производительности сети. Был проведен анализ предметной области ролевого функционирования в БСС, который показал актуальность проводимых исследований. На основании проведенного анализа работ по ролевому функционированию в беспроводных сенсорных сетях, был предложен подход к ролевому функционированию самоорганизующейся децентрализованной БСС. Предлагаемый подход включает в себя выделение четырех основных ролей узлов сети: сборщик, хранитель, анализатор и контроллер сети. Дополнительно для обеспечения безопасности сети возможно внедрение роли детектора атак, который реализует алгоритмы обнаружения атак в БСС.

Ключевые слова: беспроводная сенсорная сеть, самоорганизующаяся сеть, безопасность беспроводных сенсорных сетей, ролевое функционирования.

APPROACH TO THE ROLE-BASED MANAGEMENT OF WIRELESS SENSOR NETWORKS

Meleshko Aleksei
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS),
39, 14-th Linia, St. Petersburg, 199178, Russia
e-mail: meleshko.a@iias.spb.su

Abstract. The work is devoted to the description of the mechanisms of role-based management of various wireless sensor networks (WSN). Role management in the WSN is aimed at distributing the functions of the base station to several network nodes, which has a positive effect on network performance. The analysis of the subject area of role management in the WSN was carried out. Based on the analysis of work on role-based management in wireless sensor networks, an approach to the role-based management of a self-organizing decentralized WSN was proposed. The proposed approach includes the allocation of four main roles of network nodes: collector, custodian, analyzer and network controller. Additionally, to ensure network security, it is possible to introduce the role of an attack detector, which implements attack detection algorithms in the WSN.

Keywords: wireless sensor network, self-organizing network, security of wireless sensor networks, role-based management.

Обеспечение безопасности беспроводных сенсорных сетей (БСС) является одной из важных задач на сегодняшний день. Применение БСС в различных объектах, в том числе критически важных, порождает необходимость в разработке различных схем их построения с целью обеспечения надежности, отказоустойчивости и безопасности БСС, например, добавление в БСС свойств самоорганизации и децентрализации. Децентрализация позволяет распределить функции базовой станции сети на несколько узлов и тем самым убрать единую точку отказа системы, в случае атаки на которую работоспособность всей сети может быть нарушена. Одним из методов реализации свойства децентрализации в БСС является введение в нее механизма ролевого функционирования, то есть внедрение системы ролей для узлов БСС с возможностью динамического их перераспределения в процессе работы сети. При этом каждый конкретный узел имеет возможность выполнять определенные функции, которые определены его ролью. Для одного узла может быть заложена возможность выполнения нескольких ролей с возможностью их динамической смены. В итоге функции единой базовой станции БСС распределяются на все узлы, и выход какого-либо узла в сети не будет приводить к нарушениям в ее работе, так как функции вышедшего из строя узла будут переданы другому.

Существует ряд работ, посвященных ролевому управлению в беспроводных сенсорных сетях. Например, в работе [1] авторы описывают разработку программного обеспечения для беспроводных сенсорных сетей на базе модели с ролями узлов. Отмечается, что использование ролевой модели может повысить эффективность работы БСС. Описывается архитектура программного обеспечения, состоящая из трех уровней: уровень управления, уровень интерфейса и уровень функциональности. Уровень управления включает в себя средства для управления состоянием сети и мониторинга. Уровень интерфейса обеспечивает взаимодействие узлов между собой и с внешними устройствами. Уровень функциональности включает различные сервисы, такие как сбор, обработку и анализ данных. Каждый узел в сети на основе ролевой модели выполняет свои задачи и функции в соответствии со своей ролью. Программное обеспечение было протестировано на специальном тестовом стенде, где был развернут небольшой пример беспроводной сенсорной сети. Эксперименты подтвердили эффективность использования ролевой модели узлов. Однако, авторами не приводится описание конкретных ролей и их функционала. В [2] описывается схема организации БСС с ролевым функционированием с использованием репутации узлов при назначении им определенной роли. В зависимости от значения репутации узлу может быть назначена определенная роль. Она рассчитывается с использованием таких показателей как количество успешных передач данных конкретным узлом и количество неудачных передач или количество потерянных пакетов. Каждый раз при взаимодействии с другими узлами, проводится оценка качества их работы (репутации) и заносится в соответствующую таблицу. Таким образом, узлы с низкой репутацией не могут получить в БСС какую-либо значимую роль.

В статье [3] авторы рассматривают ролевое построение БСС. Оно основано на объединении узлов БСС с одной ролью в динамические регионы (группы). Таким образом, каждый регион генерирует свою собственную модель маршрутизации, которая может быть эффективно использована для передачи информации. Данный подход направлен на решение проблемы оптимизации БСС, возникающей в связи с ограниченными ресурсами и необходимостью передачи большого объема информации. Полученные авторами результаты показали, что их подход может существенно улучшить энергоэффективность сети и сократить необходимые ресурсы для передачи информации. Авторами выделяются следующие роли для узлов: маршрутизатор (Router), прокси (Proxy), производитель (Producer), интегратор (Integrator), инициатор (Initiator).

По результатам анализа релевантных работ можно сделать вывод, что в части работ не приводится описание конкретных ролей и их функционала, а если приводится, то роли имеют общий характер (например, роутер, прокси), не отражающий особенности распределения функций базовой станции по узлам сети. Также большинство работ имеют привязку к одной конкретной области применения БСС (например, мониторинг загрязнения воздуха в городе или на промышленных объектах).

Основными функциями, которые реализует базовая станция, являются сбор данных, отправка их на базовую станцию, обработка данных, агрегация, хранение [4]. Поэтому предлагается следующая система ролей для самоорганизующейся децентрализованной БСС: сборщик, хранитель, обработчик, контроллер. Узел-сборщик отвечает за сбор показаний сенсоров, которые подключены к нему. Также данный узел проводит предварительную их обработку и отправку на узел хранитель. Хранитель обеспечивает хранение полученных от сборщиков данных. Узел-обработчик запрашивает данные у хранителя и проводит обработку и анализ этих данных, а контроллер сети отвечает за работу сети в целом и принимает решения о реорганизации сети или перераспределении ролей в соответствии со своей моделью управления и запросами от других узлов. Система

ролевого функционирования реализуется на программном уровне, то есть на каждый узел БСС устанавливается программный компонент, который реализует функционал всех описанных ранее ролей. При инициализации работы БСС роль для каждого узла задается в файле конфигурации и в процессе работы может быть изменена в случае выполнения определённых условий (например, при невозможности выполнения текущей роли узлом).

Для обеспечения информационной безопасности самоорганизующейся децентрализованной БСС вводится дополнительная роль детектора атак. Узел с ролью детектора реализует работу алгоритмов обнаружения атак в сети. Он обеспечивает сбор необходимых для обнаружения данных, расчет признаков для обнаружения, а также реализацию самих алгоритмов обнаружения атак. В случае обнаружения атаки оператору сети выводится оповещение.

В работе была описана предлагаемая система ролевого функционирования в самоорганизующейся децентрализованной БСС. Система ролей включает в себя такие роли как сборщик, хранитель, обработчик, контроллер. Каждая роль реализуется с помощью программного компонента, который устанавливается на узлы и включает реализацию всех ролей. Подобная схема позволяет каждому узлу сменить выполняемую роль в любой момент времени по решению координатора сети. Также сама роль координатора может быть передана другому узлу. Ролевое функционирование в целом позволяет разделить основные функции базовой станции на несколько узлов сети, что обеспечивает большую гибкость и надежность работы системы, и позволяет уменьшить последствия атакующих воздействий, например, за счет передачи роли скомпрометированного узла сети другому узлу. В дальнейшем планируется провести введение дополнительной роли детектора атак, которая реализует алгоритмы сбора данных и детектирования атак на БСС.

СПИСОК ЛИТЕРАТУРЫ

1. Kochhal M., Schwiebert L., Gupta S. Role-based middleware for sensor networks, 2004. [Электронный ресурс]. URL: https://www.researchgate.net/publication/228741596 (дата обращения: 29.06.2023).
2. Sudip M., Ankur V. Reputation-based role assignment for role-based access control in wireless sensor networks // Computer Communications, 2011. Vol. 34(3). Pp. 281–294.
3. Ruairi R., Keane M. The Dynamic Regions Theory: Role Based Partitioning for Sensor Network Optimization, 2023. [Электронный ресурс]. URL: https://www.researchgate.net/publication/228530170 (дата обращения: 29.06.2023).
4. Sabet M., Naji H. R. A decentralized energy efficient hierarchical cluster-based routing algorithm for wireless sensor networks // AEU : International Journal of Electronics and Communications, 2015. Vol. 69. Issue. 5. Pp. 790-799. doi: 10.1016/j.aeue.2015.01.002.

УДК 004.056

ОБНАРУЖЕНИЕ АНОМАЛЬНОГО ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ И СУЩНОСТЕЙ В КОНТЕЙНЕРНЫХ СИСТЕМАХ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Мельник Максим Владимирович, Котенко Игорь Витальевич
СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: mkmxvh@gmail.com, ivkote@comsec.spb.ru

Аннотация. В настоящее все большую и большую актуальность приобретает задача обнаружения аномального поведения в контейнерных системах. В работе представлены результаты создания методики обнаружения аномального поведения пользователей и сущностей в контейнерных системах на основе методов машинного обучения.

Ключевые слова: информационная безопасность; обнаружение атак и аномалий; машинное обучение; контейнеры.

DETECTION OF ABNORMAL BEHAVIOR OF USERS AND ENTITIES IN CONTAINER SYSTEMS BASED ON MACHINE LEARNING METHODS

Melnik Maksim, Kotenko Igor
SPIIRAS – SPCRAS
39 14th Line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: mkmxvh@gmail.com , ivkote@comsec.spb.ru

Abstract. Currently, the task of detecting anomalous behavior in container systems is becoming more and more relevant. The paper presents the results of creating a technique for detecting anomalous behavior of users and entities in container systems based on machine learning methods.

Keywords: information security; detection of attacks and anomalies; machine learning; containers.

Одной из важных задач информационной безопасности является задача обнаружения аномального поведения пользователей и сущностей [1, 2], причем задача выявления аномального поведения в контейнерном окружении в настоящее время приобретает все большую и большую актуальность. Так, например, в ходе исследования проведенного компанией Prevasio, представлены результаты проверки порядка 4 000 000 общедоступных образов Docker, размещенных на Docker Hub. В результате было обнаружено, что более половины из них имеют критические уязвимости, а несколько тысяч образов содержат вредоносные или потенциально опасные элементы. Таким образом, компании разработчики сталкиваются с тем, что в ходе создания сервисов и технологических решений уже на начальном этапе система «заражена» и/или уязвима перед атакующими. Системы контейнеризации используются разработчиками постоянно, в том числе и для разработок

решений на объектах критической инфраструктуры. А уже после внедрения новых сервисов, цифровизации индустрии, специалисты по информационной безопаности ищут методы борьбы с атаками.

В статьях [3, 4] акцентируется внимание на угрозах APT (расширенная постоянная угроза) и корпоративных атаках. Как утверждается специалистами аналитических центров кибербезопасности (Лаборатория Касперского, Позитив Технолоджи и др.), данные атаки играют решающую роль, поскольку в настоящее время вторжение в государственный сектор и организации — обычное дело. Перспективным направлением решения задачи обнаружения аномальной активности в контейнерных системах состоит в разработке методики обнаружения аномальной активности на основе UEBA с применением методов машинного обучения с применением как традиционных методов машинного обучения [5], так и методов глубокого машинного обучения [6, 7].

В [8-9] подчеркивается важность аналитики поведения пользователей и сущностей в качестве инструмента предотвращения угроз информационной безопасности. В [10] делается акцент на трудности обнаружения неизвестного вредоносного поведения на основе UEBA из-за отсутствия помеченных данных. В [8] предлагается модель машинного обучения, основанная на поведенческой аналитике UEBA, которая более эффективно защищает пользовательские данные и предотвращает внутренние угрозы. В [9] внимание концентрируется на системе UEBA, которая позволяет отслеживать и контролировать поведение пользователей, IP-адресов и устройств на предприятии.

В ходе экспериментальных исследований в рамках проекта по выявлению аномального поведения в контейнерной среде был создан испытательный стенд, состоящий из виртуальной машины Ubuntu 22.04 и веб-сервера, развернутого в контейнерной среде. Создание наборов данных выполнялось с использованием утилиты auditd (Linux Audit Daemon). Затем были созданы и размечены данные нормальной и аномальной пользовательской активности.

За основу выявления аномалий предлагалось брать набор признаков, отражающих выполняемые процессы, сетевые вызовы, использование оперативной памяти, файловые операции и прочее. Для оценки поведения было введено два базовых понятия: норма — набор признаков, характеризирующих легальные вычислительные операции в контейнере; аномалия — набор признаков, характеризирующих не легальные, то есть вредоносные вычислительные операции в контейнере.

В дальнейшем предполагается глубокое исследование методов выявления аномального поведения в контейнерном окружении на основе методов глубокого обучения.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В., Саенко И. Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник Российской академии наук. 2014. Т. 84. № 11. С. 993-1001.
2. Котенко И. В., Ушаков И. А., Пелёвин Д. В., Преображенский А. И., Овраменко А. Ю. Выявление инсайдеров в корпоративной сети: подход на базе UBA и UEBA // Защита информации. Инсайд, 2019. № 5. С. 26-35.
3. Carlsson O., Nabhani D. User and Entity Behavior Anomaly Detection using Network Traffic // Blekinge Institute of Technology, Karlskrona. 2017. Pp. 1-52.
4. Zaid A., Al-Hamdi Ayeda G., Habeb Abduljlil A. Intelligent Machine Learning mechanism for Advanced Persistent Threats (APT) early detection // Al-Yemenia University Journal. 2020. Pp.153-188.
5. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning // IEEE Access, 2018. Vol. 6. Pp.72714-72723. DOI: 10.1109/ACCESS.2018.2881998.
6. Гайфулина Д. А., Котенко И. В. Применение методов глубокого обучения в задачах кибербезопасности. Часть 1 // Вопросы кибербезопасности. 2020. №3(37). С. 76-86. DOI: 10.21681/2311-3456-2020-03-76-86.
7. Гайфулина Д. А., Котенко И. В. Применение методов глубокого обучения в задачах кибербезопасности. Часть 2 // Вопросы кибербезопасности. 2020. № 4(38). С. 11-21. DOI: 10.21681/2311-3456-2020-04-11-21.
8. Datta J., Dasgupta R., Dasgupta S., Rohit Reddy K. Real-Time Threat Detection in UEBA using Unsupervised Learning Algorithms // 5th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech). 2021. 21508374. DOI:10.1109/IEMENTech53263.2021.9614848.
9. Shashanka M., Schwab C., Shen M., Wang J. User and Entity Behavior Analytics for Enterprise Security // IEEE International Conference on Big Data (Big Data). 2016. Pp. 1867-1874. DOI:10.1109/BigData.2016.7840805.
10. Wang Y., Guo Y., Fang. C. A semantic-based method for analysing unknown malicious behaviours via hyper-spherical variational auto-encoders // IET Information Security. Vol. 17, Issue 2, March 2023. Pp. 244-254. DOI:10.1049/ise2.12088.

УДК 004.855

ПОСТРОЕНИЕ СПАМ-ФИЛЬТРА СРЕДСТВАМИ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ

Мокрецов Никита Сергеевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, лит. Ф, Санкт-Петербург, 19702, Россия
e-mail: mokrecovnikita6374@gmail.com

Аннотация. Предлагается решение задачи построения спам-фильтра, основанного на статистических методах оценивания сообщений — байесовского фильтра, главным преимуществом которого заключается в его обучаемости. Рассматриваются признаки спам-писем, задаваемые в алгоритмах фильтрации: формальные и лингвистические и места расположения спам-фильтров: на стороне провайдер, на корпоративном сервере и на стороне клиента. Обсуждаются достоинства байесовского фильтра. Показано, что для исследования способов

повышения точности фильтрации спама применяется смещенная редуцированная оценка для статистического оценивания текста и смоделировано математическое ядро фильтра и словарь, эмулирующий подлинную базу слов.

Ключевые слова: спам-фильтр; байесовский фильтр; смещенная редуцированная оценка; словарь слов.

BUILDING A SPAM FILTER USING AN ARTIFICIAL NEURAL NETWORK

Mokretsov Nikita
Saint Petersburg Electrotechnical University «LETI»
5 Professor Popov St, lit. F, St. Petersburg, 197376, Russia
e-mail: mokrecovnikita6374@gmail.com

Abstract. A solution to the problem of constructing a spam filter based on statistical methods for evaluating messages is proposed — a Bayesian filter, the main advantage of which is its trainability. The features of spam e-mails specified in the filtering algorithms are considered: formal and linguistic, and spam filter locations: on the provider side, on the corporate server and on the client side. The advantages of the Bayesian filter are discussed. It shown that in order to study ways to improve the accuracy of spam filtering, a biased reduced estimate is used for the statistical evaluation of the text, and the mathematical kernel of the filter and a dictionary that emulates the real word base are modeled.

Keywords: spam filter; Bayesian filter; biased reduced estimate; dictionary of words.

Главной характеристикой спам-фильтра является достоверность фильтрации спама. Достоверность фильтрации — это относительная величина, вычисляемая как отношение числа выявленных фильтром спам-писем в исследуемой выборке почтовых сообщений к числу всех присутствующих в ней спам-писем [1].

Задача, которую решает детектор спама — разделить входящий поток сообщений на спам и нормальную почту. Для того чтобы произвести данное разделение или фильтрацию, детектору необходимо производить анализ всех поступающих сообщений по ряду соответствия определенным критериям. Данные критерии представляют собой признаки пришедшего письма. Эти признаки традиционно делят на четыре пространства, вычисления решений в которых производится, как правило, независимо:

1) IP-адрес сервера отправителя;
2) Оформление и стиль писем, заголовки, форматирование, характерные обороты;
3) Статистика слов в письмах;
4) Контрольные суммы («сигнатуры») текстов писем.

Решения по каждому из признаков письма соотносятся с признаками спам-писем, хранимыми, как правило, в базе данных фильтра, или заранее заданными в алгоритмах фильтрации. Существующие признаки спам-писем условно можно разделить на две группы − формальные и лингвистические. Формальные признаки включают в себя [2]:

– почтовые адреса, IP-адреса (это позволяет обеспечить фильтрацию по RBL-спискам);
– отсутствие адреса отправителя;
– отсутствие адреса получателя или наоборот наличие большого количества получателей;
– отсутствие IP-адреса в системе интернет-адресов DNS;
– определенный размер и формат сообщения;
– путь доставки электронной почты и т.п.

Лингвистические признаки включают в себя (распознавание спама по содержанию письма) [3]:

– слова и фразы, построенные определенным образом;
– эвристические признаки;
– статистические признаки.

Исходя из наиболее общих подходов, можно выделить три места расположения таких фильтров [4,5]:

– фильтрация на стороне провайдера;
– фильтрация на корпоративном сервере;
– фильтрация на стороне клиента.

Для фильтрации спама провайдеры, как правило, используют следующие методы:

1) Использованием RBL-сервисов (фильтрация по IP-адресам, которые имеют отношение к спаму: с данного IP-адреса или через таковой высылался спам, IP-адрес принадлежит провайдеру, на чьем сервере размещен сайт, рекламируемый спамом и т.п);

2) Распределенные методы обнаружения спама — сбор данных о спам-почте из максимально возможного количества точек сети. Эти данные обрабатываются и делаются доступными для всех заинтересованных участников информационного обмена.

Фильтрация спама корпоративном сервере — это системы, которые имеют возможность работать с текстом письма и не просто определять его содержимое, а уметь относить данное письмо к определенной категории, предназначенной для той или иной группы.

Большинство средних и крупных компаний имеют свой корпоративный почтовый сервер, установленный в офисе. Для них существует категория специального серверного программного обеспечения — продуктов, позволяющих фильтровать спам на почтовом сервере до рассылки его по рабочим местам сотрудников.

Фильтрация спама на рабочей станции пользователя — это когда отдельные пользователи работают с малым потоком данных. У них неизвестная, с точки зрения поставщиков антиспам-решений, производительность компьютера, отсутствие постоянной связи с Интернетом — то есть невозможно или слишком дорого постоянно «закачивать» массивы контрольных суммы писем или IP «черных дыр». Зато они могут очень точно отличить спам письма. Поэтому среди пользовательских спам-фильтров наибольшее распространение получили фильтры, основанные на статистических методах оценивания сообщений.

Главное преимущество байесовских фильтров заключается в их обучаемости. Фильтр в своем составе может и не иметь словаря русских слов. Но достаточно в течение 1-2 недель регулярно пользоваться кнопками «спам» / «не_спам» и процент отсекания спама, т.е. производительность работы фильтра, резко вырастает. Хорошие результаты всегда возникают только после постоянного и аккуратного «доучивания» системы.

В рамках данной работы для исследования способов повышения точности фильтрации спама, путем применения смещенной редуцированной оценки для статистического оценивания текста, смоделировано математическое ядро фильтра и словарь, эмулирующий подлинную базу слов. База слов представляет собой два текстовых файла определенной структуры, службами фильтра должны производиться поиск значений вероятностей для известных слов, регистрация новых и подсчет частот. Модель необходима для установления приблизительных пороговых значений и проверки правильности расчетов. Также модель позволила протестировать формулу редуцированной смещенной оценки Джеймса-Стейна именно на применимость к решению такой сугубо прикладной задачи как фильтрация спама.

Для определения пороговых значений с помощью модели фильтра использованы категорированные пользователем письма: образцы явного спама, образцы «чистой» почты и образцы «серого» спама (различные рассылки, наличие или отсутствие подписок пользователя на которые сложно установить). Из каждой категории формировалась выборка из писем. Все письма были предварительно подготовлены в виде совокупности текстовых файлов. Частотный словарь в виде двух текстовых файлов для заголовка и тела письма был подготовлен на основе набора из выборки спам-писем, который был использован при теоретическом расчете редуцированной оценки. В процессе анализа писем спам-фильтром частотный словарь не изменялся.

Далее последовательно в поля для ввода текста письма вводились заголовок и тело каждого тестового письма и на основе значений вероятностей, выбранных из частотного словаря, осуществлялся расчет.

Для тестирования использована другая выборка спам-писем по набору слов достаточно схожих с теми, для которых производился расчет пороговых значений. Аналогичным образом сформированы выборки из писем «серого» спама и писем «чистой почты». Для обучения фильтра использовался набор из 500 спам-писем.

СПИСОК ЛИТЕРАТУРЫ

1. Татарникова Т. М. Статистические методы исследования сетевого трафика // Информационно-управляющие системы. 2018. № 5 (96). С. 35-43.
2. Мироненко А. Н. Метод распознавания спам-сообщений на основе анализа заголовка письма // Математические структуры и моделирование. 2010. Вып. 21. С.133-140.
3. Катасёв А. С., Катасёва Д. В., Кирпичников А. П. Нейросетевая технология классификации электронных почтовых сообщений // Вестник технологического университета. 2015. Т. 18, № 5. С. 180-183.
4. Советов Б. Я., Колбанёв М. О., Татарникова Т. М. Оценка вероятности эрланговского старения информации // Информационно-управляющие системы. 2013. № 6 (67). С. 25-28.
5. Бескид П. П., Татарникова Т. М. О некоторых подходах к решению проблемы авторского права в сети интернет // Ученые записки Российского государственного гидрометеорологического университета. 2010. № 15. С. 199-210.

УДК 004.056

МЕТОД ОБНАРУЖЕНИЯ АНОМАЛЬНОЙ АКТИВНОСТИ И НАРУШЕНИЙ КРИТЕРИЕВ И ПОЛИТИК БЕЗОПАСНОСТИ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Новикова Евгения Сергеевна[1], Кузнецов Михаил Дмитриевич[2]
[1] СПИИРАН – СПб ФИЦ РАН
14 линия, 39, Санкт-Петербург, 199178, Россия
e-mail: novikova@comsec.spb.ru
[2]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова, ул., 5, Санкт-Петербург, 197022, Россия
e-mail: mkuznetsov7991@gmail.com

Аннотация. Цифровизация, усложнение информационных и киберфизических систем и расширение спектра передаваемых данных имеют как положительные, так и негативные стороны, в частности, рост числа уязвимостей и, как следствие, увеличение рисков хищения и повреждения данных. В данной работе представлен комбинированный подход к выявлению аномальной активности и нарушений политик безопасности на основе потоков событий, который сочетает методы выявления аномалий во временных рядах и анализ графовых структур. В предложенном методе предлагается использовать не только статистические характеристики событий, но и качественные, такие как их взаимосвязь и очередность.

Ключевые слова: обнаружение аномалий; аномальная активность; политики безопасности; анализ временных рядов.

A METHOD FOR DETECTING ANOMALOUS ACTIVITY AND VIOLATIONS OF SECURITY CRITERIA AND POLICIES IN REAL TIME

Novikova Evngenia[1], Kuznetsov Mikhail[2]
[1]SPIIRAS – SPCRAS
39 14th Line St, Petersburg, 199178, Russia
e-mail: novikova@comsec.spb.ru
[2]Saint-Petersburg Electrotechnical University «LETI»
5 Professora Popova st., St. Petersburg, 197022, Russia
e-mail: mkuznetsov7991@gmail.com

Abstract. Digitalization, the complication of information and cyber-physical systems and the expansion of the range of transmitted data have both positive and negative sides, in particular, an increase in the number of vulnerabilities and, as a result, an increase in the risk of data theft and damage. Based on related studies, this paper presents a combined approach to detecting anomalous activity and violations of security policies based on event streams. In the proposed method, it is proposed to use not only statistical characteristics, but also qualitative ones, such as the relationship of events and sequence.

Keywords: anomaly detection; abnormal activity; privacy policies; time series analysis.

Стремительный рост цифровизации имеет две стороны, одна из них повышение производительности труда, сбор и анализ данных для оптимизации и контроля выполнения процессов и множество других возможностей, другая — образует возможности иного характера, для хищения и повреждения данных. Для выявления аномалий в потоке событий в условиях реального времени разработаны различные подходы. В настоящем докладе рассматривают методы на основе машинного обучения и анализа процессов.

Рассматриваемый подход к выявлению аномалий на политиках безопасности состоит их двух компонентов. Первый компонент выполняет анализ событий с учетом временного контекста, и в его основе лежит концепция множества временных окон, предложенная в [1].

Предлагается использовать три различных временных окна: окно контекста (предыстория), окно наблюдения (поступающие события, причем данное окно захватывает много меньший интервал, чем окно контекста) и общее окно (их совокупность). Преобразованные данные временных рядов с помощью обученных кодировщиков представляются в виде векторов одинаковой длины, которые в свою очередь рассматриваются как координаты в многомерном пространстве.

Далее определяется расстояние от точки контекста до общей и наблюдаемой точек. Если наблюдаемая точка находится вне гиперсферы, радиус которой определен как расстояние от точки контекста до общей точки, то наблюдаемое окно классифицируется аномальным.

Следует отметить, что в данном случае происходит оценка лишь количественных характеристик системы, при этом теряются данные о взаимосвязи тех или иных событий, а также о контексте данных, что является важным для определения несоответствия политикам безопасности. Метод поддерживает несколько вариантов приложения, как обучение с учителем, так и обучение без учителя, что говорит о его высокой применимости в условиях отсутствия размеченных обучающих выборок.

В основе второго компонента лежит анализ процессов и их представление в виде графов, меняющихся во времени. Для анализа динамики изменения графов используется метод, предложенный в [2]. Его основой служит математическая модель, описывающая граф в виде набора переходов, представленных в виде кортежей. Исходя из количества связей, а также набора вершин, которые они связывают происходит расчет схожести графовых структур. Метод является применимым для потока событий высокой плотности, так как вычислительная сложность является полиномиальной. Однако его применение требует наличия достоверных и корректных в точки зрения структуры процессов наборов данных.

Предложенный метод выявления аномальной активности и нарушений критериев и политик безопасности включает в себя традиционные этапы анализа данных, направленных на решение поставленной задачи, такие как предобработка входных данных (нормализация, стандартизация), классификация объекта, представленного вектором или матрицей атрибутов, и выдача решения о статусе объекта (норма/не норма).

Таким образом методика выявления аномальной активности и нарушений критериев и политик безопасности на основе аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности состоит из 4 основных этапов:

- извлечения признаков из потока событий,
- построение модели нормального поведения,
- обнаружение аномалий,
- объяснение полученных результатов.

Основной акцент в докладе делает на способы извлечения признаков из потока событий для формирования контекста событий и связей между ними. Для тестирования предложенного подхода авторы используются набор событий ОС, собранных в течение двух месяцев национальной лабораторией Лос Аламос, США [3].

Исследование выполнено за счет гранта Российского научного фонда (проект № 21-71-20078).

СПИСОК ЛИТЕРАТУРЫ

1. Chris U. Carmona and François-Xavier Aubet and Valentin Flunkert and Jan Gasthaus, Neural Contextual Anomaly Detection for Time Series, 2021, doi: https://doi.org/10.48550/arXiv.2107.07702.

2. Abd E. K., A simple graph embedding for anomaly detection in a stream of heterogeneous labeled graphs : Pattern Recognition / Abd Errahmane Kiouche, Sofiane Lagraa, Karima Amrouche, Hamida Seba. Volume 112, 2021. ISSN 0031-3203, [Электронный ресурс]. URL: https://doi.org/10.1016/j.patcog.2020.107746 (дата обращения 30.06.2023).
3. Набор событий ОС Unified Host and Network Data Set, [Электронный ресурс]. URL: https://csr.lanl.gov/data/2017/ (дата обращения 30.06.2023).

УДК 004.056

КОНСИСТЕНТНАЯ БЕЗОПАСНОСТЬ СИСТЕМ УПРАВЛЕНИЯ БОЛЬШИМИ ДАННЫМИ

Полтавцева Мария Анатольевна, Калинин Максим Олегович, Зегжда Дмитрий Петрович
Санкт-Петербургский политехнический университет Петра Великого,
Политехническая ул., 29, Санкт-Петербург, 194064, Россия,
e-mails: poltavtseva@ibks.spbstu.ru, max@ibks.spbstu.ru, dmitry@ibks.spbstu.ru

Аннотация. Рассматриваются современные системы больших данных и новые задачи их информационной безопасности. Обосновывается необходимость универсального консистентного представления данных и процессов, предлагается новая математическая модель данных и направления по решению задач безопасности систем управления большими данными на ее основе.

Ключевые слова: информационная безопасность; большие данные; безопасность больших данных; управление данными; системный анализ; модель данных.

CONSISTENCY SECURITY OF BIG DATA MANAGEMENT SYSTEMS

Poltavtseva Maria, Kalinin Maxim, Zegzhda Dmitry
The Peter the Great St. Petersburg Polytechnic University,
29 Polytechnicheskaya St., St. Petersburg, 194064, Russia
e-mails: poltavtseva@ibks.spbstu.ru, max@ibks.spbstu.ru, dmitry@ibks.spbstu.ru

Abstract. Modern systems of big data and new problems of their information security are considered. The need for a universal consistent representation of data and processes is justified, a new mathematical model of data and directions for solving security problems of big data management systems on its basis are proposed.

Keywords: information security; big data; big data security; data management; system analysis; data model.

Системы управления большими данными сегодня воспринимаются в различном ключе, или, иными словами, на различных уровнях [1-2].

С точки зрения бизнес-логики, большие данные — это значимые наборы информации из различных источников. Управление их сбором, хранением и обработкой в такой трактовке — высокоуровневый бизнес-процесс.

С точки зрения инженерии данных, ключевой является гетерогенная среда обработки данных включающая поли-базы данных и «потоковые» инструменты. В терминологии этой области, система управления большими данными — совокупность инструментов сбора, обработки, хранения и использования (включая анализ) больших данных, каждый из которых решает свою специальную задачу.

На нижнем уровне такого представления находится инфраструктура больших данных, включая решения виртуализации, центры обработки данных и т.д.

На каждом из приведенных уровней рассмотрения, с точки зрения информационной безопасности, можно выделить различные угрозы: от возможности логического вывода до аппаратных «закладок».

Консистентный подход к безопасности систем управления большими данными предполагает, в соответствии с общими принципами системного анализа и теории систем, учет безопасности на всех уровнях взаимодействия, от инструментального (в общем, случае, начиная от оборудования) до семантического. Такое рассмотрение систем управления большими данными позволяет систематизировать задачи безопасности в отношении этого класса решений.

С уровнями рассмотрения систем управления данными соотносятся и угрозы информационной безопасности, и методы защиты от них. На уровне инфраструктуры (назовем его — уровень инфраструктуры) каждый узел распределенной системы управления данными представляет собой вычислительный компонент обработки информации, реализованный физически или с применением среды виртуализации. В данном случае надо отметить, что спектр угроз и методов защиты в системах управления большими данными не отличается от любых других распределенных систем и узлов.

На уровне инструментов управления (назовем его — уровень управления), если рассматривать традиционные системы управления базами данных, основные атаки на сами данные ставят целью, в первую очередь, нарушение их конфиденциальности или целостности [3].

Эти угрозы реализуются через нарушение политики безопасности путем инъекции в язык запросов или использования недостатков контроля доступа иными способами. При этом борьба с внутренним, доверенным нарушителем остается существенной проблемой. Для систем больших данных указанные проблемы усугубляются следующими факторами:

– Отдельные средства контроля доступа у каждого инструмента (при наличии) не согласованные между собой.
– Отсутствие согласованного аудита для выявления и расследования инцидентов.
– Снижение степени доверия к среде управления данными.

Все эти факторы обусловлены такими свойствами инструментов обработки больших данных, как незрелость, распределенность (в том числе, географическая), разнородность. При этом разнородность инструментов приводит как к увеличению числа администраторов (доверенных пользователей) различных узлов системы, а значит — числа потенциальных нарушителей, так и к большим уязвимостям системы контроля доступа, за счет использования различных не согласованных между собой систем разграничения доступа, зачастую — на основе различных моделей безопасности.

В основе проблемы согласования управления доступом на уровне инструментов системы управления большими данными лежит различная грануляция данных в компонентах систем больших данных [4]. Готовых эффективных решений преодоления данной проблемы на сегодня неизвестно. Преодолеть такую разнородность можно используя общее представление данных для всех инструментов системы на над-инструментальном, концептуальном уровне обработки информации (предполагая инструментальный уровень — логическим в рамках архитектуры ANSI/SPARK). Для этого, учитывая взаимосвязь между структурами данных и операциями над ними, необходима разработка соответствующей модели данных [5-6].

Перспективной математической основой такой модели концептуального уровня является теория множеств и подход на основе агрегатов. Это обуславливается общим математическим базисом для систем управления базами данных (СУБД) в составе поли-баз данных систем управления большими данными, также относящемуся к этому разделу математики [2-3].

Важной задачей остается аудит процессов обработки данных и построение адекватных моделей конкретных систем управления большими данными для учета их индивидуальных особенностей и оценки реализации контроля доступа. Для решения этой задачи может использоваться как аудит журналов инструментов обработки, так и наложенные решения и фреймворки на основе технологий распределенного реестра.

На уровне бизнес-логики (назовем его — уровень использования) можно говорить об угрозах мошенничеств путем воздействия на данные, если рассматривать ее как модификацию доверенным пользователем, а также об угрозе inference — атак или угрозе непрямого логического вывода над данными. Обнаружение этого вида атак к тому же затруднено отсутствием нарушения политики безопасности со стороны злоумышленника при их реализации.

На этом уровне к большим данными применяются различные методы обеспечения конфиденциальности: обезличивание (или анонимизация), зашумление данных, криптографическая обработка путем хэширования для сокрытия идентификаторов.

Сегодня показано, что полная защита от логического вывода является np-полной задачей и перечисленные методы защиты направлены в первую очередь на снижение вероятности проведения атаки. Основной механикой, которая может быть применена для прогнозирования возможного логического вывода, является математическое моделирование взаимосвязей данных на основе функциональных зависимостей.

Сегодня этот раздел реляционной теории используется для проектирования пост-реляционных хранилищ данных с минимальной избыточностью, однако уже показано его использование для анализа каналов вывода в СУБД [7].

В итоге стоит сказать, что обеспечение безопасность информации в системах управления большими данными является комплексной задачей, которую следует рассматривать, в соответствии с консистентным подходом, на различных уровнях, в соответствии с представлением самой системы.

Исследование выполнено за счет гранта Российского научного фонда № 23-11-20003, https://rscf.ru/project/23-11-20003/ Грант Санкт-Петербургского научного фонда (Соглашение №23-11-20003 о предоставлении регионального гранта).

СПИСОК ЛИТЕРАТУРЫ

1. Константинов А., Кузнецов С., Скворцов Н. Ценность ваших данных. М.: Альпина PRO, 2022. 574 с.
2. Есу М. Т, Вальдуриес П. Принципы организации распределенных бах данных. М.: ДМК Пресс. 2021. 678 с.
3. Полтавцева М. А. Безопасность баз данных : учеб. пособие для студентов высших учебных заведений, обучающихся по УГСН 10.00.00 «Информационная безопасность» по программам подготовки бакалавров, магистров, специалистов. СПб : ФГАООУ ВО Санкт-Петербургский политехнический университет Петра Великого, 2023. 143 с. ISBN 978-5-7422-8008-8. EDN RICQEN.
4. Colombo P., Ferrari E. Access control technologies for Big Data management systems: literature review and future trends // Cybersecur. 2019. Vol. 2. № 3. 13 p.
5. Грей П. Логика, алгебра и базы данных. М.: Машиностроение, 1989. 368 с.
6. Цикритзис Д., Лоховски Ф. Модели данных. М.: Финансы и статистика, 1985. 344 с.
7. Полтавцев А. А., Хабаров А. Р., Селянкин А. О. Сравнительный анализ методов защиты от логического вывода // Проблемы информационной безопасности. Компьютерные системы. 2020. № 4. С. 17-25. EDN ALWWPF.

УДК 004.056

СБОР ДАННЫХ ЦИФРОВОЙ КРИМИНАЛИСТИКИ ДЛЯ ЦЕЛЕЙ THREAT HUNTING

Попков Илья Александрович[1], Котенко Игорь Витальевич[2]
[1]Университет ИТМО
[2]СПИИРАН – СПб ФИЦ РАН,
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: popkov.ilya.alexandrovich@yandex.ru, ivkote@comsec.spb.ru

Аннотация. Современные методы проактивного поиска угроз (threat hunting) требуют большого объема данных об инфраструктуре и происходящих в ней событиях. Однако, поток данных, не задействованных в обнаружении инцидентов, понижает продуктивность SIEM-систем, в которых используются методы проактивного поиска угроз. В работе рассмотрены подходы к измерению информативности собираемых данных в случае применения автоматизированного сбора данных цифровой криминалистики.

Ключевые слова: информационная безопасность; проактивный поиск угроз, цифровая криминалистика.

DIGITAL FORENSICS DATA GATHERING FOR THREAT HUNTING PURPOSE

Popkov Ilya [1], Kotenko Igor [2]
[1]ITMO University
[2] SPIIRAS – SPCRAS
39 14th line Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: popkov.ilya.alexandrovich@yandex.ru, ivkote@comsec.spb.ru

Abstract. Modern methods of proactive threat hunting require large amounts of data about the infrastructure and the events occurring in it. However, the flow of data not involved in incident detection reduces the productivity of SIEM systems, which use proactive threat detection methods. This paper considers approaches to measuring the informativeness of the collected data in the case of automated digital forensics data gathering.

Keywords: information security, threat hunting, digital forensics.

Одной из актуальных задач информационной безопасности является анализ защищенности информационных и телекоммуникационных систем [1-3] и проактивный анализ угроз (threat hunting) [4-5].

Threat hunting (TH) нацелен на обнаружение продвинутых атак (advanced persistent threat, APT), обошедших имеющиеся в инфраструктуре средства защиты [4]. Данная методика предполагает, что система уже скомпрометирована и предлагает методы по выявлению индикаторов компрометации.

Одним из этапов проведения TH является сбор цифровых следов, которые могут подтверждать или опровергать выдвинутую гипотезу о компрометации инфраструктуры. Документирование как можно большего объема происходящих в инфраструктуре событий позволит команде аналитиков быстрее и точнее детектировать проникновение, а, следовательно, пресечь его на более ранних этапах [5-6]. Однако объем собираемых данных влечет за собой проблемы снижения эффективности средств мониторинга [7].

Путем анализа собираемых данных и изменения вовлеченности типов событий и типов информации о системе можно определить набор необходимых для сбора событий/информации. Построение зависимости типов собираемой информации от занимаемого ими объема и полной или частичной задействованности в последующих расследованиях киберинцидентов позволят повысить эффективность систем мониторинга в целом и процесса TH в частности.

В данной работе предлагается метод измерения данной зависимости и алгоритм настройки конвейера журналирования на основании проводимых измерений. В работе предлагается подход к расчету количества информации, которую необходимо обработать для подтверждения той или иной гипотезы компрометации, исходя из количества и качества собираемых событий / информации, их нормализации и агрегации, размера окна корреляции событий. Подобный расчет должен определить целесообразность сбора данных цифровой криминалистики различных типов в целях проведения TH.

Дальнейшим развитием данной работы должен стать эксперимент, сравнивающий результаты описанного расчета с реальными результатами сбора данных цифровой криминалистики.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Kotenko I. Agent-Based Modeling and Simulation of Cyber-Warfare between Malefactors and Security Agents in Internet // 19th European Simulation Multiconference «Simulation in wider Europe». ECMS 2005. Riga, Latvia, 1–4 June 2005. P. 533-543.
2. Котенко И. В., Степашкин М. В., Богданов В. С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы, 2006. № 2, С.7-24.
3. Kotenko I., Doynikova E. Security Assessment of Computer Networks based on Attack Graphs and Security Events // Lecture Notes in Computer Science. 2014. Vol. 8407. P. 462-471.
4. Охота за угрозами: зачем она нужна : материалы конференции CyberPolygon, 2020. [Электронный ресурс]. URL: https://cyberpolygon.com/ru/materials/threat-hunting-why-might-you-need-it/ (дата обращения: 07.07.2023).
5. Gao P. Enabling Efficient Cyber Threat Hunting With Cyber Threat Intelligence / P. Gao, F. Shaoy, X. Liu, X. Xiaoy [et al] // IEEE 37th International Conference on Data Engineering (ICDE), IEEE. 2020. P.193-204. DOI: 10.1109/ICDE51399.2021.00024.
6. Araujo F., Kirat D., Shu X., Taylor T., Jang J. Evidential Cyber Threat Hunting // ArXiv abs/2104.10319, 2021. P.1-12. DOI: 10.48550/arXiv.2104.10319.
7. Jaeger D., Cheng F., Meinel C. Accelerating Event Processing for Security Analytics on a Distributed In-Memory Platform // 16th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC'2018), IEEE, 2018. Pp. 634-643. DOI: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00114.

УДК 004.056

СИСТЕМАТИЗАЦИЯ И ОБОБЩЕНИЕ СОБЫТИЙ БЕЗОПАСНОСТИ

Пучков Владимир Викторович[1], Едемская Екатерина Дмитриевна[2]
[1] СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
[2] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mail: puchkov-81@bk.ru, ekaterina.edemskaya51@gmail.com

Аннотация. В данной работе представлена методика, которая обеспечивает автоматическую систематизацию и обобщение оповещений для расследования киберинцидентов.

Ключевые слова: защита информации; событие безопасности; группировка событий; центр обеспечения безопасности; динамический граф.

SYSTEMATIZATION AND GENERALIZATION OF SECURITY EVENTS

Puchkov Vladimir[1], Puchkov Vladimir[2]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line St., St. Petersburg, 199178, Russia
[2] St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich
22 Bolshevikov Av., 1, St. Petersburg, 193232, Russia
e-mail: puchkov-81@bk.ru, ekaterina.edemskaya51@gmail.com

Abstract. This paper presents a technique that provides automatic systematization and generalization of alerts for the investigation of cyber incidents.

Keywords: information protection; security event; grouping of events; security center; dynamic graph.

Организации сталкиваются с постоянно растущими рисками, связанными с угрозами информационной безопасности. Разнообразие и объем предупреждений являются ошеломляющими для корпоративных центров управления безопасностью (SOC), которые располагают ограниченными ресурсами [1, 2] Для обнаружения внешних атак или внутренних угроз продукты и службы безопасности разрабатывают комплексные наборы индикаторов риска (или правил), которые выдают предупреждения о сетевых и облачных событиях. Некоторые индикаторы риска основаны на фактах и сопоставляют события с сигнатурами; например, предупреждают о совпадении строки или хэш-кода. Некоторые индикаторы риска описывают поведение сетевых объектов и помечают события, если они являются аномальными по отношению к изученным профилям [3, 4].

Распространенной практикой обработки предупреждений является простое применение ручных фильтров для отбора предупреждений, которые считаются ценными для аналитиков. У такого подхода есть очевидный недостаток — отсутствие автоматизации. Несмотря на то, что существуют исследовательские работы по машинному обучению в области управления оповещениями, результаты агрегирования оповещений, кластеризации и корреляции не имеют семантических меток, легко понятных аналитикам SOC. В то же время некоторые коммерческие системы группируют оповещения по блокам в виде логических единиц оповещений для каждого пользователя и для фиксированного временного окна. Данный подход не объясняет, почему тот или иной случай заслуживает внимания, и не учитывает тот факт, что некоторые атаки не всегда ограничиваются фиксированными границами пользователя или времени [5, 6].

Предполагается, что решением данной проблемы будет разработка методики, которая обеспечивает построение графа с динамической привязкой и систематизацией предупреждений к учетным записям пользователей и хостам для формирования готовых к расследованию случаев с временными рамками, описывающими этапы потенциальных атак, основанных на нормативных документах РФ. При таком подходе предупреждения сначала будут объединяться в логические временные блоки. Направленные связи между блоками будут устанавливаться автоматически на основе сопоставления атрибутов, обычно выполняемом при ручном расследовании, а также понимания жизненного цикла атаки. Связанные компоненты графа идентифицируются как случаи для расследования. Различные атрибуты соединенных компонентов могут использоваться для фильтрации и определения приоритетов.

СПИСОК ЛИТЕРАТУРЫ

1. Miloslavskaya N. Security operations centers for information security incident management // IEEE 4th International Conference on Future Internet of Things and Cloud. 2016. Pp. 131-136.
2. Lin T. A. Data Triage Retrieval System for Cyber Security Operations Center. 2018. 50 c.
3. Lin D., Li A., Foltz R. BEAM: An Anomaly-Based Threat Detection System for Enterprise Multi-Domain Data // IEEE International Conference on Big Data. 2020. Pp. 2610-2618.
4. Котенко И. В., Ушаков И. А. Использование технологии больших данных для мониторинга инцидентов информационной безопасности // Региональная информатика (РИ-2016) : материалы конференции. 2016. С. 168-169.
5. Bialas A., Michalak M., Flisiuk B. Anomaly detection in network traffic security assurance // International Conference on Dependability and Complex Systems. Cham: Springer International Publishing, 2019. Pp. 46-56.
6. Виткова Л. А., Паращук И. Б., Саенко И. Б. Проблематика и особенности процедур аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности в инфокоммуникационных сетях и системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная науч-техничю и науч-метод. конфер. Санкт-Петербург, 2022. С. 279-283.

УДК 004.75: 004.056

СНИЖЕНИЕ УЯЗВИМОСТИ СРЕДСТВ ПРОГРАММИРОВАНИЯ В РАЗЛИЧНЫХ СИСТЕМНЫХ СРЕДАХ ИНФОРМАЦИОННЫХ СИСТЕМ

Соничев Александр Викторович, Щиголева Марина Андреевна, Виноградов Алексей Борисович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: avson@mail.ru, vvcehanovsky@mail.ru, abvinogradov@etu.ru

Аннотация. Рассматривается подход объектно-ориентированного и системного программирования для информационной системы с логической моделью предметной области. Все решения логического, процедурного, объектно-ориентированного и системного программирования рассмотрены с позиций стандарта со сводом норм и правил применения мер обеспечения информационной безопасности.

Ключевые слова: информационная система, объектно-ориентированное программирование, уязвимости средств программирования, стандарт обеспечения информационной безопасности.

REDUCING THE VULNERABILITY OF PROGRAMMING TOOLS IN VARIOUS SYSTEM ENVIRONMENTS OF INFORMATION SYSTEMS

Sonichev Aleksandr, Zorin Kirill. Shchigoleva Marina, Vinogradov Aleksey
Saint Petersburg Electrotechnical University
5 Professora Popova st., St. Petersburg, 197376, Russia
e-mail: avson@mail.ru, vvcehanovsky@mail.ru, abvinogradov@etu.ru

Abstract. The approach of object-oriented and system programming for an information system with a logical domain model is considered. All solutions of logical, procedural, object-oriented and system programming are considered from the standpoint of a standard with a set of norms and rules for the application of information security measures.

Keywords: information system, object-oriented programming, vulnerabilities of programming tools, information security standard.

Программно-технические средства, допускающие гибкую оперативную модификацию предметных задач, реализуются декларативным языком программирования. Применимость технических решений должна соответствовать и не противоречить действующим стандартам информационной безопасности для информационных технологий, методов и средств обеспечения безопасности. Все решения логического, процедурного, объектно-ориентированного и системного программирования подпадают под действие стандарта. В описательном языке программирования, используемом для решения задач, в которых действуют объекты и отношения между этими объектами, подразумевается использование специфических применений вычислительной техники: понимание естественного языка, базы знаний, экспертные системы, интерфейсные сервисы. Информационная система и среда ее применения описывает логическую модель предметной области, знания свойств предметной области, отношения между этими свойствами, правила вывода новых свойств и отношений из уже заданных, представление о компонентах информационной системы и организационные свойства реализации предметных задач информационной системы. Язык в такой логике программирования оперирует правилами, фактами, запросами.

Вычислительная часть функциональных заданий выполняется по запросам к базе знаний информационной системы, на которые система логического программирования генерирует ответы «истина» и «ложь», выводит конкретные данные в подтверждение истинности обобщённых сведений и правил вывода, что удобно применимо для интерфейсного сервисного обслуживания [1].

Язык программирования должен быть применим в профессиональных информационных системах, быть реализован для операционных систем и мобильных платформ, поддерживаемым стандартами безопасности, иметь расширения и диалекты, стыкуемые с сохранением защищенности информационной системы [2].

Для предметно-ориентированных информационных систем актуальным требованием является наличие оперативной модификации предметных задач. При распознавании отклонений от состояния ситуации, внешней среды или архитектуры системы, предметные задачи могут претерпевать регламентированные изменения, систему коммуникационных связей, состав данных и разделов бах данных. При поддержании полноценного функционирования системы программно-технические решения и инструментальная база их поддержки должны оперировать понятиями и возможностями искусственного интеллекта [3], компьютерной лингвистики, нечислового программирования. Соответствующие им программные средства реализуют элементы математической логики [4], логического программирования, методологию проектирования и анализа экспертных систем, аппарат систем принятия решений, сервисный и интерфейсный аппарат баз знаний.

С целью выявления и предотвращения уязвимостей в языках программирования в системах гарантированного обеспечения безопасности, защиты, фиксации факторов возникновения уязвимостей, необходимо промоделировать весь комплекс задач и связей системы в методологии их программно-технической реализации. Удобным с точки зрения охвата широкого перечня задач и комплексных средств поддержки их на этапах проектирования, отладки и реализации, является декларативный язык программирования Пролог. Все запросы к базе знаний информационной системы, пройдут процедуру логического программирования с генерируемыми ответами «истина» и «ложь», выводом конкретных данных в подтверждение истинности обобщённых сведений и правил вывода, что полностью отвечает требованиям предметно-ориентированной модификации и соблюдения установленных форм интерфейсного сервисного обслуживания. Применяемый язык программирования должен обеспечить механизмы преобразований в понятиях интеллектуальных агентов, императивного программирования, интеллектуальных процедур обработки информации [5]. Кроме того, Пролог реализован для операционных систем семейства и мобильных платформ Unix, Windows, Java, NETOC, которые также поддерживаются стандартами методов и средств обеспечения безопасности информационных технологий, допускающих подключения расширений и диалектов [6]. На возможностях языка Пролог возможна организация

предметно-ориентированной модификации за счет замены изначального содержания понятий языка на новое смысловое содержание. При этом Предикаты языка переименовываются в Задачи для обозначения задач, которым в Прологе соответствуют предикаты. Термы этих предикатов будут пониматься как исходные данные и требуемые результаты решения этих задач, унификация предикатов будет доказательством принадлежности соответствующей задачи искомому решению.

Процесс поиска последовательности решений элементарных подзадач будет достигнут путем соответствующих подстановок, в отличии от выполняемого процесса получения пустого дизъюнкта по правилу резолюции. Отсутствие унификатора при подстановке покажет отсутствие решения известной задачи на заданных значениях исходных данных, которые вообще бы позволяли получить требуемый результат [7]. При унифицированном средстве программирования в различных системных средах информационных систем, опробованном, например, на декларативном языке программирования Пролог, можно выстроить комплексную политику снижения уязвимости языка программирования, в которой с применением «интуитивно понятного языка программирования» из «совокупности «интуитивно убедительных» умственных построений» [7] формируется интуитивная логика решений.

При организации подобной преемственности программного обеспечения удаётся обеспечить требуемую стандартами «безопасную разработку» в части создания безопасного сервиса, архитектуры, программного обеспечения и самой системы, в которой по действующей политике безопасной учтены аспекты: безопасность в методологии разработки программного обеспечения, безопасности в жизненном цикле разработки программного обеспечения, безопасность среды разработки; в ходе проектирования обозначены контрольные точки по проверке безопасности в рамках основных этапов проекта. При обслуживании информационной системы такой программной организации удаётся в высокой степени организовать обход уязвимостей, их нахождение и исправление, безопасность в управлении версиями системы и их приложениями, что отвечает квалификационным требованиям разработчиков избегать, находить и исправлять уязвимости, находить методы безопасного программирования в отношении новых разработок, их версий и модификаций.

СПИСОК ЛИТЕРАТУРЫ

1. Ездаков А. Л. Логическое программирование. БИНОМ. Лаборатория знаний, 2011. 118 с.
2. Сергиевский Г. Е., Волченков Н. А. Функциональное и логическое программирование. Academia, 2010. 320 с.
3. Сидоркина И. Г. Системы искусственного интеллекта. КноРус, 2017. 245 с.
4. Игошин В. А. Математическая логика. Изд-во Инфра-М. 2019. 399 с.
5. Игошин В. А. Теория алгоритмов. Изд-во Инфра-М. 2019. 318 с.
6. Адаменко А., Кучуков А. Логическое программирование и Visual Prolog (с CD). СПб.: БХВ-Петербург, 2003. 990 с.
7. Kolmogoroff A. Zur Deutung der intuitionistischen Logik. «Math. Zeitschrift». № 35, 1932 // К толкованию интуиционистской логики. Избранные труды. Математика и механика / Колмогоров А. Н. М., 1985. С. 142-148.

УДК 004.056.53

БЛОЧНОЕ ШИФРОВАНИЕ С ГЕНЕРАТОРОМ СЛУЧАЙНЫХ ЧИСЕЛ КАК ОСНОВА ДЛЯ ПСЕВДОВЕРОЯТНОСТНОГО ШИФРОВАНИЯ

Татчина Яна Александровна, Уваров Кирилл Андреевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
e-mails: mondikovay@gmail.com, uvarovkirill73@gmail.com

Аннотация. Рассматриваются схемы вероятностного шифрования в качестве основы для преобразования в схему псевдовероятностного шифрования при атаках с принуждением.

Ключевые слова: блочное шифрование; атака с принуждением; псевдовероятностное шифрование.

BLOCK ENCRYPTION WITH A RANDOM NUMBER GENERATOR AS A BASIS FOR DENIABLE ENCRYPTION

Tatchina Iana, Uvarov Kirill A.
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197022, Russia
e-mails: mondikovay@gmail.com, uvarovkirill73@gmail.com

Abstract. Probabilistic encryption schemes are considered as a basis for transformation into a pseudo-probabilistic encryption scheme for duress attacks.

Keywords: block encryption; coercive attack; deniable encryption.

Псевдовероятностное (отрицаемое) шифрование, в рамках криптографического способа обеспечения секретности сообщения, позволяет отправителю после передачи зашифрованного сообщения раскрыть его содержимое и ключ шифрования, в случае, если отправитель подвергся принуждающей атаке со стороны лица, который имеет возможность прямого воздействия на отправителя и/или получателя. При этом мы предполагаем, что были перехвачены все сообщения, которые были переданы в ходе сеанса связи. Схемы такого шифрования реализуются так, что отправитель и/или получатель раскрывают данные, но не секретные, а фиктивные, и протокол отрицаемого шифрования не должен вызывать сомнений, что в переданном шифртексте не содержится

какое-либо другое сообщение, отличающееся от раскрытого фиктивного сообщения. В симметричных алгоритмах шифрования отправитель и получатель разделяют ключи на секретный и на фиктивный и в случае атаки раскрывают только фиктивный ключ. В асимметричных алгоритмах, когда отправитель шифрует по открытому ключу получателя, возможность обмана достигается тем, что в ходе протокола отрицаемого шифрования обе стороны обмениваются разовыми открытыми ключами, которые используются для согласования разового секретного ключа для скрытного шифрования секретного сообщения [1-4].

В известной схеме [5] для вероятностного блочного шифрования используется b-битовая функция шифрования, а зашифрованное сообщение разделяется на v-разрядные блоки данных. Для преобразования блока открытого сообщения генерируется u-битовый случайный блок, за которым следует составление b-битового входного блока данных, где происходит конкатенация двух двоичных векторов и вычисляется блок зашифрованного сообщения с ключом шифрования. На практике в устройствах шифрования используется генератор случайных чисел, который должен быть внедрен в качестве внутренней части, который реализует алгоритм блочного шифрования. Безопасность повышается только в том случае, когда у противника нет возможности модифицировать генератор случайных чисел или его выходные данные.

Схема вероятностного блочного шифрования может быть преобразована в схему псевдослучайного блочного шифрования, которую можно использовать для одновременного кодирования двух независимых сообщений (секретного и фиктивного) с использованием двух ключей (секретного и фиктивного) [6]. Для этого можно заменить генератор случайных чисел некоторой блочной функцией шифрования. Вместо генерации v-битного случайного числа будет v-битный блок секретного сообщения. При использовании блочного алгоритма шифрования для преобразования блока секретного сообщения с секретным ключом, полученный промежуточный блок шифртекста является вычислительно неотличимым от равномерно случайного v-битового двоичного вектора. Затем блок этот блок объединяется с блоком фиктивного сообщения и преобразуется в выходной блок зашифрованного сообщения.

При принуждении отправитель и получатель сообщения могут открывать фиктивное сообщение и поддельный ключ и объявлять об использовании блочного вероятностного алгоритма шифрования. Таким образом, во время принуждающей атаки обе стороны имеют возможность без подозрений использовать фиктивные данные, т. е. предлагаемый псевдо-вероятностный метод шифрования обеспечивает отрицаемость. В монографии [5] представлены несколько методов вероятностного шифрования с некоторой детерминированной функцией блочного шифрования. Для каждого из этих методов можно предложить соответствующую псевдо-вероятностную схему блочного шифрования, которая безопасна для атак с принуждением. Такие псевдо-вероятностные схемы шифрования относятся к запланированным алгоритмам и протоколам отрицаемого. Они обеспечивают двунаправленную защиту до тех пор, пока противник не сможет проверить время расшифровывания, необходимое для раскрытия секретного сообщения. Если у него есть такая возможность, то он сможет установить, что время дешифрования поддельного сообщения меньше времени дешифрования секретного сообщения. Кроме того, можно предположить, что в некоторых случаях противник сравнивает функции кодирования, используемых для дешифрования фиктивных и секретных сообщений.

Чтобы обеспечить отрицаемость во время атак, совершаемых противником, имеющим указанные возможности, можно предложить следующий дополнительный критерий алгоритма шифрования: фиктивные и секретные сообщения должны быть расшифрованы одним и тем же алгоритмом дешифрования.

СПИСОК ЛИТЕРАТУРЫ

1. Moldovyan A. A., Moldovyan N. A. Practical Method for Bi-Deniable Public-Key Encryption // Quasi groups and related systems. 2014. Vol. 22. Pp. 277-282.
2. Moldovyan N. A. Berezin A. N., Kornienko A. A., Moldovyan A. A., Bi-deniable Public-Encryption Protocols Based on Standard PKI // Proceedings of the 18thFRUCT & ISPIT Conference, 18-22 April 2016, Technopark of ITMO University, Saint-Petersburg, Russia. FRUCT, Finland. Pp 212-219.
3. Молдовян Н. А., Михтеев М. С., Нгуен Ким Туан Протокол отрицаемого шифрования по открытому ключу, включающий процедуру аутентификации пользователей // Вопросы защиты информации. 2016. № 3. С. 9-15.
4. Михтеев М. С., Молдовян Н. А. Гибридный протокол отрицаемогошифрования, основанный на процедуре аутентификации // Вопросы защиты информации. 2017. № 1. С. 12-17.
5. Moldovyan N. A., Moldovyan A. A. Innovative cryptography // Boston ; Massachusetts: Charles River Media, 2006. Pp. 386.
6. Молдовян Н. А., Биричевский А. Р., Мондикова Я. А. Отрицаемое шифрование на основе блочных шифров // Информационно управляющие системы. № 5. 2014. С. 80-86.

УДК 004.056

РАЗРАБОТКА КИБЕРФИЗИЧЕСКОГО СТЕНДА ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ ПРОМЫШЛЕННЫХ СИСТЕМ ОЧИСТКИ ВОДЫ

Федорченко Елена Владимировна, Новикова Евгения Сергеевна, Данилов Александр Сергеевич
СПИИРАН – СПб ФИЦ РАН
14 линия В. О., 39, 199178, Санкт-Петербург, Россия
e-mails: doynikova@comsec.spb.ru, novikova@comsec.spb.ru, aleksandrsdanilov@gmail.com

Аннотация. Наличие цифровых систем мониторинга и управления технологическими процессами, такими как очистка воды, создает возможности для кибератак, которые могут иметь катастрофические последствия для

экологии. Для анализа защищенности киберфизических промышленных систем очистки воды в работе разрабатывается киберфизический стенд, имитирующий такую систему.

Ключевые слова: кибербезопасность; системы очистки воды; стенд.

DESIGNING CYBER PHYSICAL TESTBED TO ANALYSE CYBER SECURITY

Fedorchenko Elena, Novikova Evgenia, Danilov Alexandr
SPIIRAS – SPCRAS
39 14th line V. I., St. Petersburg, 199178, Russia
e-mails: doynikova@comsec.spb.ru, novikova@comsec.spb.ru, aleksandrsdanilov@gmail.com

Abstract. Digital systems for monitoring and controlling technological processes such as water treatment create opportunities for cyberattacks, which can have catastrophic consequences for the environment. To analyze the security of cyber physical water treatment systems, the authors develop a cyber physical testbed simulating such a system.

Keywords: cyber security; water treatment system; cyber physical testbed.

Кибератаки, направленные против промышленных систем очистки воды, могут привести к загрязнению воды химическими веществами и, как следствие, к нанесению вреда окружающей среде и здоровью людей. В то же время промышленным компаниям это может нанести также огромный материальный ущерб. В последнее время активность киберпреступников против систем очистки воды выросла [1]. Поэтому задача обеспечения защищенности таких систем является актуальной.

В данной работе рассматриваются вопросы разработки киберфизического стенда для анализа защищенности промышленных систем очистки воды. Такой стенд необходим для сбора данных от сенсоров, а также сетевого трафика, в случае нормального и аномального, например, в результате успешных кибератак, протекания процессов очистки воды. Собранные данные могут использоваться для разработки методов выявления кибератак и аномалий на основе машинного обучения [2].

Существуют различные типы очистки воды: (1) механическая очистка (отстаивание, флотация, фильтрация); (2) биологическая очистка (аэробная, анаэробная); (3) физико-химическая (адсорбция; мембрана; сепарация; ионный обмен; флокуляция; химическое окисление). В данном исследовании за основу берется физический стенд, имитирующий механическую очистку путем флотации [3].

Процесс флотации включает следующие этапы: смешивание и подача воды; флокуляция (включает коагуляцию, собственно флокуляцию, созревание флокулы и контроль pH); аэрация; флотация и удаление осадка с поверхности воды. В работе предлагается расширить данный физический стенд за счет системы управления и сбора данных (Supervisory Control And Data Acquisition, SCADA). За основу предлагается взять стенд SWaT, разработанный в Центре исследований кибербезопасности при Университете Технологии и Дизайна г. Сингапур [4]. Для каждого процесса предлагается добавить программируемые логические контроллеры (ПЛК). Датчики и актуаторы процесса будут передавать данные на ПЛК с помощью кольцевой сети. SCADA система и ПЛК будут соединены с помощью звездообразной сети.

Система SCADA позволит записывать данные с ПЛК. Стенд предлагается расширить следующими датчиками: датчик температуры; pH-анализатор; датчик веса; датчик уровня; датчик расхода; датчик загрязняющих веществ; датчик плотности воды; измеритель давления.

Следует отметить, что, хотя некоторые из этих датчиков присутствуют в испытательном стенде (а именно, датчик уровня, расходомер, pH-анализатор, преобразователь потока и измеритель давления), они не могут передавать данные в систему SCADA.

Разработанный стенд далее будет использоваться для исследования в области анализа защищенности, включающего следующие этапы: разработка обычного метода сбора данных (в нормальном режиме работы системы и при проведении кибератак); проведение атак и сбор данных; валидация собранного набора данных; анализ данных для разработки методов выявления атак и аномалий.

Таким образом, в данной статье авторы предложили подход к разработке киберфизического стенда для анализа защищенности промышленных систем очистки воды. В настоящее время авторы имеют доступ к физическому стенду, который будет расширен до киберфизического на основе предложенного подхода. Киберфизический стенд будет использоваться для проведения тестовых кибератак, сбора данных и разработки методов выявления кибератак аномалий.

Исследование выполнено за счет гранта Российского научного фонда и гранта Санкт-Петербургского научного фонда № 23-11-20024, https://rscf.ru/project/23-11-20024/, в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Новости BBC [Электронный ресурс]. URL: https://www.bbc.com/news/world-us-canada-55989843.am (дата обращения: 30.06.2023).
2. Lemay A. Fernandez J. M. Providing SCADA Network Data Sets for Intrusion Detection Research // 9th Workshop on Cyber Security Experimentation and Test (CSET 16). USENIX Association: Austin, TX. 2016.
3. Kyzas G. Z., Matis K. A. Flotation in Water and Wastewater Treatment. 2018. № 6. Pp. 116. [Электронный ресурс]. URL: https://doi.org/10.3390/pr6080116 (дата обращения: 30.06.2023).
4. Goh J., Adepu S., Junejo K. N., Mathur A. A Dataset to Support Research in the Design of Secure Water Treatment Systems // CRITIS 2016: Critical Information Infrastructures Security. International Conference on Critical Information Infrastructures Security: conference paper, 2016. Pp. 88–99.

УДК 004.056.5

РАССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ КАК ОСНОВА ОПЕРАТИВНОГО АНАЛИЗА КИБЕРБЕЗОПАСНОСТИ И ИСТОЧНИК ИСХОДНЫХ ДАННЫХ ДЛЯ АРХИТЕКТУРНЫХ КОМПОНЕНТОВ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Федорченко Елена Владимировна, Чечулин Андрей Алексеевич, Паращук Игорь Борисович
СПИИРАН – СПб ФИЦ РАН,
14-я линия В. О., 39, Санкт-Петербург, 194064, Россия,
e-mails: elenadoynikova@mail.ru, chechulin@comsec.spb.ru, shchuk@rambler.ru

Аннотация. Рассматриваются современные аспекты и процедурные особенности расследования компьютерных инцидентов. Предложены новые инновационные подходы к расследованию компьютерных инцидентов, результаты которого являются основой для оперативного анализа кибербезопасности и источником исходных данных для всех архитектурных компонентов единой системы аналитической обработка больших массивов гетерогенных данных о событиях кибербезопасности, включая компоненты оперативного анализа и управления рисками информационной безопасности.

Ключевые слова: компьютерные инциденты, расследование, компьютерная атака, информационная безопасность, компонент, архитектура, управление рисками.

INVESTIGATION OF COMPUTER INCIDENTS AS A BASIS FOR OPERATIONAL ANALYSIS OF CYBERSECURITY AND A SOURCE OF SOURCE DATA FOR ARCHITECTURAL COMPONENTS OF INFORMATION SECURITY RISK MANAGEMENT

Fedorchenko Elena, Chechulin Andrey, Parashchuk Igor
SPIIRAS – SPCRAS
39, 14-th Linia, V.I., St. Petersburg, 199178, Russia
e-mails: elenadoynikova@mail.ru, chechulin@comsec.spb.ru, shchuk@rambler.ru

Abstract. Modern aspects and procedural features of investigation of computer incidents are considered. New innovative approaches to the investigation of computer incidents are proposed, the results of which are the basis for operational analysis of cybersecurity and a source of initial data for all architectural components of a unified analytical system for processing large arrays of heterogeneous data on cybersecurity events, including components of operational analysis and information security risk management.

Keywords: computer incidents, investigation, computer attack, information security, component, architecture, risk management.

Принято считать, что смысл понятий «компьютерное преступление» (КП) и «компьютерный инцидент» (КИ) различен. Вместе с тем, существующие подходы к их расследованию, а также используемые для этого алгоритмы и методы не только похожи, но и используют одни механизмы исследований. Более того, применяемые методики и сопутствующие процедуры расследования КП и КИ во многом опираются на одни и те же исходные данные. Иногда симбиоз КП и КИ называют общим термином — «компьютерная преступность» (computer crime) или «киберпреступность» (cyber crime). Данное понятие трактуется как любое действие, в котором инструментом, целью или местом преступных действий являются компьютерные системы [1, 2].

В рамках ГОСТ Р ИСО/МЭК 27001:2006 выделяются следующие виды КИ (или инцидентов информационной безопасности): утрата услуг, оборудования или устройств; системные сбои или перегрузки; ошибки пользователей; несоблюдение политики или рекомендаций по информационной безопасности; нарушение физических мер защиты; неконтролируемые изменения систем; сбои программного обеспечения и отказы технических средств, а также нарушение прав (правил) доступа [3].

При этом расследование КИ включает в себя комплексные работы по сбору, анализу данных, экспертизе вычислительных систем, сетей, носителей информации и фиксации свидетельств неправомерного проникновения в ИТ-инфраструктуру организации [1, 2, 4].

Расследование КИ направлено на полную ликвидацию угрозы безопасности корпоративным данным, а также на выявление инициатора вредоносных действий, определение последствий произошедшего и формирование стратегии построения защиты корпоративных сетей (включая защиту пользователей в рамках социальных сетей) от будущих компьютерных атак [4-6].

Классические расследования КИ включают этапы: выявление инцидентов информационной безопасности; локализация угрозы и блокировка нежелательных последствий инцидента; сбор и анализ доказательств; выявление виновных и установление причин КИ; ликвидация последствий инцидента, а также анализ результатов расследований в целях недопущения повторений КИ [4].

Новые предложенные инновационные методы, модели, методики и алгоритмы проведения расследований КИ используют результаты интеллектуальной аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности. Эти результаты ориентированы на поиск (с заданной оперативностью, точностью и полнотой) источников и времени возникновения компьютерных атак. На основе проведенного анализа, оригинальных решений и разработанной общей верхнеуровневой архитектуры, разработаны и используются модели, методы и алгоритмы проведения расследований КИ, которые способны реализовывать

общий подход к расследованию в виде последовательности этапов: извлечение данных; извлечение фактов; анализ отдельных фактов; построение общей картины произошедшего инцидента [7, 8].

При этом на этапе извлечения данных формируется общий пул, в который попадут как данные от хостовых систем журналирования, так и сведения от сетевых систем безопасности. Эти данные защищены от модификации путем расчета цифровых подписей или контрольных сумм. На втором этапе из сформированного пула данных с помощью специальных алгоритмов формируются наборы фактов (в форме, определенной в моделях данных). С использованием этих фактов на третьем этапе проводится анализ отдельных фактов для установления их корректности и сочетаемости с другими фактами. На четвертом этапе отдельные проверенные факты с установленными взаимосвязями собираются вместе в единую картину произошедшего КИ с помощью методики построения комплексного представления состояния системы во время инцидента. Все перечисленные этапы представляют собой элементы комплексного метода проведения расследований КИ на основе аналитической обработки больших массивов гетерогенных данных о кибербезопасности.

Результаты расследования КИ являются основой для оперативного анализа кибербезопасности и, одновременно, источником исходных данных для архитектурных компонентов единой системы аналитической обработка больших массивов гетерогенных данных о событиях кибербезопасности, например, таких как компоненты обнаружения в реальном времени атак на основе имитационного и графо-ориентированного моделирования, компоненты обнаружения в реальном времени аномальной активности и нарушений критериев и политик безопасности, компоненты оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов, компоненты оперативной визуализации больших массивов гетерогенных данных о событиях кибербезопасности, а также компонентов оперативного анализа и управления рисками информационной безопасности.

Особого внимания, на наш взгляд, заслуживают вопросы использования результатов расследований КИ в качестве исходных данных для задач оперативного анализа и управления рисками информационной безопасности на основе аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности [8, 9].

С учетом важности и содержания результатов расследований КИ, для компонентов оперативного анализа и управления рисками информационной безопасности на основе аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности, разработана функциональная архитектура, включающая уровень планирования задач, связанных с обработкой событий, анализа и управления рисками, и уровень анализа и управления рисками. Данные уровни архитектуры этих компонентов учитывают также весь набор контролируемых параметров кибербезопасности, которые могут понадобиться для систем управления информационной безопасностью и событиями безопасности (SIEM-систем) [10, 11].

В рамках архитектуры этих компонентов выделены функциональные модули: модуль формирования интегральной оценки риска в статическом режиме; модуль формирования интегральной оценки риска в динамическом режиме; модуль сравнения интегральной оценки с критерием и модуль постановки задачи компоненту поддержки принятия решений. В рамках данной архитектуры и с учетом результатов расследований КИ также определены связи с другими компонентами системы (компоненты сбора данных, оценки рисков, обнаружения атак и обнаружения аномалий, и поддержки принятия решений), а также высокопроизводительным кластером для выполнения вычислительных задач.

Таким образом, рассмотрены современные аспекты, процедурные особенности и предложены новые инновационные подходы к расследованию КИ, результаты которых являются основой для оперативного анализа кибербезопасности и источником исходных данных для всех архитектурных компонентов единой системы аналитической обработка больших массивов гетерогенных данных о событиях кибербезопасности, включая компоненты оперативного анализа и управления рисками информационной безопасности.

Работа выполнена при финансовой поддержке гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Энсон С. Реагирование на компьютерные инциденты. Прикладной курс / пер.с англ. Д. А. Беликова. М.: ДМК Пресс, 2021. 436 с.
2. Мандиа К., Просис К. Защита от вторжений. Расследование компьютерных преступлений. М.: Лори, 2005. 467 с.
3. Национальный стандарт ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ. 2008. 62 с.
4. Васильева И. Н. Расследование инцидентов информационной безопасности : учебное пособие. СПб.: Изд-во СПбГЭУ, 2019. 113 с.
5. Kolomeets M., Benachour A., El Baz D., Chechulin A., Strecker M., Kotenko I. Reference architecture for social networks graph analysis // Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications, 2019. Vol. 10, № 4. Pp. 109-125.
6. Doynikova, E. V., Kotenko I. V. Countermeasure selection based on the attack and service dependency graphs for security incident management // Lecture Notes in Computer Science. Vol. 9572. Springer, 2016. Pp. 107-124.
7. Дойникова Е. В., Котенко И. В. Оценка защищенности и выбор мер противодействия для управления кибербезопасностью : монография. М. : Изд-во РАН. 2021. 184 с.
8. Дойникова Е. В., Котенко И. В. Методики и программный компонент оценки рисков на основе графов атак для систем управления информацией и событиями безопасности // Информационно-управляющие системы. 2016. № 5. С. 54-65.
9. Дойникова Е. В., Котенко И. В., Чечулин А. А. Динамическое оценивание защищенности компьютерных сетей в SIEM-системах // Безопасность информационных технологий. 2015. № 3. С. 33-42.
10. Kotenko I. V., Parashchuk I. B. Specification of Quality Indicators for Security Event and Incident Management in the Supply Chain // International Journal of Computing, 2021. Vol. 20, Issue 1. Pp. 22-30.
11. Kotenko I. V., Parashchuk I. B. Synthesis of Controlled Parameters of Cyber-Physical-Social Systems for Monitoring of Security Incidents in Conditions of Uncertainty // 3rd Annual International Conference on Information System and Artificial Intelligence (ISAI2018) 22–24 June 2018, Suzhou, China // IOP Conf. Series: *Journal of Physics: Conference Series (JPCS).* Vol. 1069 (2018) 012153. Pp. 1-6.

УДК 004.056

ПРИМЕНЕНИЕ ДИНАМИЧЕСКОЙ ЧЕТЫРЕХЭТАПНОЙ МОДЕЛИ ЗАЩИТЫ ДАННЫХ, ОСНОВАННОЙ НА КРИПТОГРАФИИ И СТЕНОГРАФИИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Хлебоказов Виталий Алексеевич, Кушнир Дмитрий Викторович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mail: vhlebokazov@gmail.com, dmitry.kushnir@gmail.com

Аннотация. В работе рассматривается возможность применения четырехэтапной модели защиты данных в сфере облачных вычислений.

Ключевые слова: кибербезопасность; облачные вычисления; криптография; стеганография; модель безопасности; конфиденциальность.

APPLICATION OF A DYNAMIC FOUR-STAGE DATA PROTECTION MODEL BASED ON CRYPTOGRAPHY AND SHORTHAND IN CLOUD COMPUTING

Khlebokazov Vitaly, Kushnir Dmitry
St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich
22 Bolshevikov Av., 1, St. Petersburg, 193232, Russia
e-mail: vhlebokazov@gmail.com, dmitry.kushnir@gmail.com

Abstract. The paper considers the possibility of applying a four-stage data protection model in the field of cloud computing.

Keywords: cybersecurity; cloud computing; cryptography; steganography; security model; privacy.

Развитие технологий облачных вычислений в современном мире высоких технологий происходит достаточно стремительно, так как все больше компаний предпочитают использовать сервисы облачных вычислений. Это связано с тем, что они являются гибким, надежным и масштабируемым инструментом и во многих случаях данные решения наиболее доступны в реализации.

Применение облачных вычислений заключается в возможности предоставления доступа к общим и динамически настраиваемым ресурсам через компьютерную сеть по требованию. Такой подход позволяет пользователям получать доступ к ресурсам компьютерной системы, включая хранилища данных и вычислительную мощность, по мере необходимости, не тратя ресурсы на их непосредственное управление.

Целью работы является рассмотрение возможности разработки модели безопасности данных при использовании облачных вычислений. Предполагается, что работа модели будет основана на методах криптографии, стенографии и будет направлена на решение таких проблем безопасности и конфиденциальности как: потеря и кража данных, манипулирование [1-3]. В ходе исследования предполагается: идентифицировать существующую проблему; определить требования к разрабатываемой системе; определить параметры оценки эффективности применения. Для разработки модели будет использован язык программирования Python.

Предлагаемая к разработке четырехэтапная модель защиты данных будет основываться на RSA, расширенном стандарте шифрования и алгоритмах шифрования на основе идентификационных данных вместе со стеганографией младших разрядов, что обеспечит защиту данных и их безопасность [4-5]. Четыре этапа включают в себя использование алгоритмов шифрования, стеганографии, резервного копирования и восстановления данных, а также совместное использование данных.

СПИСОК ЛИТЕРАТУРЫ

1. Erl T., Puttini R., Mahmood Z. Cloud Computing: Concepts, Technology & Architecture. The Pearson Service Technology Series from Thomas Erl. London: Pearson, 2013. 1st ed. 528 p.
2. Шемякин С. Н., Ахметшина М. Э., Катасонов А. И., Манкаев Р. М. Выяснение криптографических свойств булевых функция шифра «магма» // Экономика и качество систем связи. 2021. №1 (19). С. 67-73.
3. Paar C., Pelzl J., Preneel B. Understanding Cryptography. A Textbook for Students and Practitioners. Heidelberg: Springer-Verlag, 2010. 1st ed. 382 p.
4. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы Криптографии. М.: Гелиос АРВ. 2002. 480 с.
5. Лось А. Б., Нестеренко А. Ю., Рожков М. И. Криптографические методы защиты информации для изучающих компьютерную безопасность: учеб. для академического бакалавриата. 2-е изд., испр. М.: Юрайт, 2019. 473 с.

УДК 004.056

ПОДХОД К ФОРМИРОВАНИЮ ПРИЗНАКОВ ЦЕЛЕВОЙ КИБЕРАТАКИ ДЛЯ АТРИБУЦИИ КИБЕРНАРУШИТЕЛЯ

Хмыров Семен Сергеевич, Котенко Игорь Витальевич
СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: khmyrov.s.s@gmail.com, ivkote@comsec.spb.ru

Аннотация. Различные кибернарушители отличаются уровнем подготовки при реализации целевых кибератак (APT) прежде всего на стратегическом и технико-тактическом уровнях. В данной работе представлен подход к формированию данных о кибернарушителях, их возможностях, применяемых техниках и тактиках.

Ключевые слова: кибербезопасность, целевые атаки, критическая инфраструктура, продвинутые постоянные угрозы, атрибуция кибернарушителя.

APPROACH TO FORMING THE FEATURESOF A TARGET CYBER ATTACK FOR ATRIBUTION OF THE CYBER INTERRUPTER

Khmyrov Semyon, Kotenko Igor
SPIIRAS – SPCRAS
14th Line, V. I., 39, St. Petersburg, 199178, Russia
e-mails: khmyrov.s.s@gmail.com, comsec.spb.ru

Abstract. Various cyber intruders differ in the level of training in the implementation of targeted cyber attacks (APT), first of all, at the strategic and technical-tactical levels. This paper presents an approach to generating data on cyber intruders, their capabilities, techniques and tactics used.

Keywords: cybersecurity, targetedattacks, criticalinfrastructure, advancedpersistentthreats, attribution ofcyberintruders.

Процесс атрибуции кибернарушителя при реализации целевых атак на объекты критической информационной инфраструктуры (КИИ) включает последовательные действия по расследованию инцидента (связанной цепочки событий, инцидентов), формированию доказательной базы, анализу техник, тактик и процедур (ТТП), отличительной специфики APT, сравнения полученного результата с существующими профилями кибернарушителей (банком данных) [1-3].

Проблематика. Одной из особенностей целевой кибератаки является сложность выявления данного типа атак. В большинстве случаев информация становится доступной после длительного времени, когда все цели были достигнуты и жизненный цикл атаки окончен [4].

Определение вторжения (кибератаки) происходит в полуавтоматическом режиме и после ее осуществления; атаки APT в большинстве случаев имеют скрытый характер и трудно обнаружимы [5].

Одним из способов решения данной проблемы, является идентификация кибератаки (целевой атаки на КИИ) по ее признакам.

Формирование признаков целевой кибератаки. Как было определенно выше, целевая атака (APT) имеет жизненный цикл (несколько шагов реализации) [6] и набор ТТП [7]. Обращаясь к [7, 8], можно сформировать набор данных, позволяющих по установленным индикаторам выявлять реализацию целевой кибератаки, производить корреляцию и обогащение событий [9-12].

Анализируя [13], определим признаки для целевой атаки.

Рассмотрим пример определения признаков на различных этапах [14]:

Этап 1. Первоначальный доступ (InitialAccess).

– T1190 (использование уязвимостей общедоступных приложений);
– T1566 (фишинг);
– .001 (целевой фишинг с вложением).

Этап 2. Выполнение (Execution).

– T1059 (использование интерпретаторов командной строки и сценариев).
– .003 (при помощи командной строки Windows);
– .005 (использование полезных нагрузок VisualBasic для выполнения вредоносных команд).
– T1569 (злоупотребление системными службами для выполнения команд или программ).
– .002 (путем внедрения в диспетчер управления служб Windows).
– T1053 (использование метода функционального планирования задач для упрощения выполнения вредоносного кода).
– .005 (при помощи планировщика задач Windows).

Данная цепочка действий содержит описание подозрительного (деструктивного) поведения в информационной среде и может являться признаком целевой кибератаки [14, 15].

Применяя платформы [11, 12], сформированные индикаторы интегрируются в процесс обнаружения кибератаки (угроз).

Представленный в работе подход, основанный на формировании признаков кибератаки позволяет в режиме реального времени следить за состоянием защищенности целевой инфраструктуры и идентифицировать деструктивное воздействие, формировать собственную базу индикаторов атак, определять таксономию атрибутов для целевой кибератаки и выявлять взаимосвязи между ними.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Le R. M. The Problems with Seeking and Avoiding True Attribution to Cyber Attacks // Sans: [сайт]. [Электронный ресурс]. URL: https://www.sans.org/blog/the– problems– with– seeking– and– avoiding– true– attribution– to– cyber– attacks (дата обращения: 06.07.2023).
2. Lemay A., Calvet J., Menet F., Fernandez J. M. Survey of publicly available reports on advanced persistent threat actors // Computers & Security. 2018. Vol. 72. Pp. 26-59.
3. Котенко В. И., Саенко И. Б., Коцыняк М. А., Лаута О. С. Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей // Труды СПИИРАН. 2017. № 6(55). С. 160-184.
4. Хмыров С. С., Котенко И. В. Анализ расширенной модели «cyberkillchain» для атрибуции нарушителей кибербезопасности при реализации целевых атак на объекты критической инфраструктуры // XII Санкт-Петербургская межрегиональная конференция ИБРР-2021. 2021. С. 103-105.

5. Котенко И. В., Хмыров С. С. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак // Вопросы кибербезопасности № 4, 2022. С. 52-79. DOI:10.21681/2311-3456-2022-4-52-79.
6. Котенко И. В., Степашкин М. В., Богданов В. С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы, 2006. № 2. С. 7-24.
7. MITRE ATT&CK: Enterprise Matrix // The MITRE Corporation [Электронный ресурс]. URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения: 07.07.2023).
8. MITRE ATT&CK: ICS Matrix // The MITRE Corporation [Электронный ресурс]. URL: https://attack.mitre.org/matrices/ics/ (дата обращения: 07.07.2023).
9. Caltagirone S., Pendergast A., Betz C. The Diamond Model of Intrusion Analysis // www.threatintel.academy: [сайт]. [Электронный ресурс]. URL: https://www.threatintel.academy/wp-content/uploads/2020/07/diamond-model.pdf (дата обращения: 07.07.2023).
10. The Unified Kill Chain [Электронныйресурс]. URL: https://unifiedkillchain.com/ (дата обращения: 04.07.2023).
11. Seker E. Cyber Threat Intelligence Understanding Fundamentals. 2019.
12. Gylling A. Enriching Attack Models with Cyber Threat Intelligence. Masters Theses // Digitala Vetenskapliga Arkivet [Электронный ресурс]. URL: https://www.diva–portal.org/smash/record.jsf?dswid=– 467&pid=diva2%3A1477504 (датаобращения: 07.07.2023).
13. Earth Baku: An APT Group Targeting Indo-Pacific Countries [Электронный ресурс]. URL:https://documents.trendmicro.com/assets/white_papers/wp-earth-baku-an-apt-group-targeting-indo-pacific-countries.pdf (дата обращения: 03.07.2023).
14. Kaspersky Anti Targeted Attack Platform, Using indicators of compromise (IOC) and attack (IOA) for Threat Hunting. [Электронный ресурс]. URL: https://support.kaspersky.com/KATA/3.7/en-US/194907.htm (дата обращения: 05.07.2023).
15. Anashkin Y., Zhukova M. About the System of Profiling User Actions Based on the Behavior Model // IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). 2021. Pp. 191-195. DOI: 10.1109/ElConRus51938.2021.9396158.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

УДК 004.032.26

АНАЛИЗ ПРОБЛЕМЫ ОБРАБОТКИ ДАННЫХ БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Авраменко Владимир Семенович, Чичков Евгений Сергеевич
Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: vsavr@yandex.ru, jen.chichckow2014@yandex.ru

Аннотация. В докладе проведен анализ проблемы обработки данных беспилотными летательными аппаратами. Предложен вариант решения поставленной задачи с использованием внедрения методов машинного обучения на борту беспилотного летательного аппарата. Сформулированы основные достоинства такого подхода. Рассмотрены существующие готовые портативные аппаратные решения, разработанные специально для работы с нейронными сетями.

Ключевые слова: беспилотный летательный аппарат, технологии машинного обучения, сбор данных, передача данных, обработка данных, нейронные сети.

ANALYSIS OF THE PROBLEM OF DATA PROCESSING BY UNMANNED AERIAL VEHICLES BASED ON MACHINE LEARNING METHODS

Avramenko Vladimir, Chichkov Evgeny
Military Academy of Communications Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails: vsavr@yandex.ru, jen.chichckow2014@yandex.ru

Abstract. The report analyzes the problem of data processing by unmanned aerial vehicles. A variant of solving the problem is proposed using the introduction of machine learning methods on board an unmanned aerial vehicle. The main advantages of this approach are formulated. The existing ready-made portable hardware solutions designed specifically for working with neural networks are considered.

Keywords: unmanned aerial vehicle, machine learning technologies, data collection, data transmission, neural networks.

Использование роботизированных систем на сегодняшний день стало ключевым фактором в различных сферах деятельности. С помощью новых технологий автоматизации, используемых в роботизированных системах, значительно повышается эффективность решения широкого спектра задач высокой сложности, зачастую ранее трудно выполнимых. Особенно активно развиваются беспилотные летательные аппараты.

Под беспилотным летательным аппаратом (БПЛА) понимается летательное средство, не имеющее на своем борту экипажа. Также используется более широкое понятие − беспилотная летательная система (БПЛС), которая включает в себя:

– собственно БПЛА;
– средства управления БПЛА (автоматизированное рабочее место, пульт оператора);
– средства связи с БПЛА (например, средства радио или спутниковой связи);
– дополнительное оборудование, необходимое для перевозки или обслуживания БПЛА.

БПЛА имеют ряд значимых достоинств по сравнению с другими видами летательных аппаратов:

1. Высокая мобильность и маневренность. Размеры и конструкция БПЛА позволяют легко и беспрепятственно исследовать сложные объекты в самых различных условиях.

2. Доступность относительно небольших БПЛА. Например, современные БПЛА вертолетного типа (так называемые коптеры) имеют низкую стоимость и не сложны в производстве.

3. Простота управления. Обучение новых операторов происходит в короткие сроки и не требует больших ресурсов.

В настоящее время БПЛА общего назначения в основном выполняют функции наблюдения, обнаружения объектов различного рода, сбора данных и транспортировки грузов. При организации сетей (роев) эти функции могут выполняться крайне эффективно. Например, скоординированные усилия позволят транспортировать груз, который не способен поднять один БПЛА. Другой пример — распределенный рой способен одновременно собирать и обрабатывать информацию о множестве объектов и обмениваться полученными данными по принципу децентрализованных сетей [1].

В последние годы активно развиваются и БПЛА военного назначения. Соответствующие разработки в военной сфере ведутся в России. Система управления малыми БПЛА для массированного удара «Стая-93», разработанная военно-учебным научным центром ВВС России, была представлена на форуме «Армия-2019» еще в 2019 году [2].

Несмотря на все свои положительные качества и достоинства ход успешного выполнения задач БПЛА во-многом зависит от оператора. Однако, данную проблему можно решить путем внедрения технологий машинного обучения на основе нейронных сетей как в систему управления БПЛА, так и в оборудование, реализующее целевые функции БПЛА. Благодаря такой модернизации беспилотные аппараты смогут самостоятельно достигать поставленных целей. Например, БПЛА может самостоятельно производить обработку видеоданных и выполнять распознавание объектов без участия человека.

Под обработкой данных понимаются все этапы преобразования данных к конечному результату, а именно: очистка, редактирование, форматирование и т.п. Производить необходимые вычисления можно различными способами: посредством человека (вручную), удаленно на стационарных вычислителях, на борту БПЛА.

Важно отметить возможность производить обработку собранных данных непосредственно на борту БПЛА. Такой подход к решению поставленной проблемы обладает существенными преимуществами, особенно в задачах, требующих получение результатов в близком к реальному масштабу времени.

Во-первых, отсутствует необходимость передавать по каналам связи большой объем необработанных данных, что в конечном счете значительно сокращает время получения оператором конечных результатов. Кроме того, снижаются требования к средствам связи и передачи данных по пропускной способности. Во-вторых, у оператора БПЛА появляется возможность управлять одновременно несколькими БПЛА или выполнять другие задачи.

В общем случае использование технологий машинного обучения на основе искусственных нейронных сетей в БПЛС, связанных со сбором и обработкой данных, позволяет повысить оперативность доведения конечных результатов потребителям, в ряде случаев повысить точность результатов, сократить затраты на персонал. Более того, при организации роевых беспилотных летательных систем, в которых в режиме реального времени одни БПЛА для выполнения своих функций используют результаты сбора и обработки данных, выполненными другими БПЛА, обработка данных на борту становится безальтернативной.

Вместе с тем реализация обработки данных на борту требует вычислительного устройства достаточной производительности, дополнительного электропитания, что влечет за собой увеличение массогабаритных показателей, отрицательно влияет на летные характеристики (скорость, высота, продолжительность полета). Также повышаются требования к информационной безопасности БПЛА, так появляются дополнительные риски перехвата или потери уже обработанной информации. Также конкуренты (противник) будут стараться получить информацию о методах и средствах обработки. Необходимо предусмотреть дополнительные меры защиты средств аппаратного, программного, математического и информационного обеспечения, передаваемых данных.

Вместе с тем, следует заметить, что большие вычислительные мощности требуются на этапе обучения искусственных нейронных сетей, и этот этап может выполняться «на земле», например, на стационарном или мобильном центре обработки данных [3]. А бортовая ЭВМ БПЛА может реализовать только задачу распознавания, не требующей существенных вычислительных ресурсов.

Самый популярный тип аппаратуры в общем случае для работы с нейронными сетями — это графические процессоры. Они способны проводить вычисления параллельно, что в значительной мере ускоряет обработку данных и тренировку новых моделей. Существуют также специальные процессоры (ASICs), которые разработаны для работы с нейронными сетями. Они позволяют получать высокую скорость работы при минимальном энергопотреблении. Для работы с нейронными сетями могут использоваться популярные фреймворки и библиотеки, например: PyTorch, TensorFlow и Keras. Они позволяют быстро разрабатывать и обучать новые модели, а также управлять аппаратурой и эффективно проводить вычисления на ней.

На данный момент одним из примеров использования технологий машинного обучения на борту БПЛА является тяжелый ударный беспилотник С-70 «Охотник». Данный аппарат способен выполнять вычисления на борту благодаря сопроцессору с элементами VLIW (very long instruction word) и SIMD (single instruction, multiple data) архитектур [4]. Однако, С-70 «Охотник» имеет массу порядка 20 тонн, и проблема размещения вычислительного комплекса для обработки данных на борту для него не так актуальна, как для небольших БПЛА массой до 5 кг.

Для БПЛА ближнего действия можно использовать уже существующие готовые портативные аппаратные решения, которые были разработаны специально для работы с нейронными сетями. На сегодня самые популярные из них Google Coral (США) и NVidia Jetson nano (США). Данные разработки являются закрытыми, что обусловливает актуальность исследований методов, средств и технологий обработки данных на борту БПЛА на основе машинного обучения.

Таким образом, перспективным путем решения проблемы обработки данных на борту микро- и мини-БПЛА является разработка модели машинного обучения на основе искусственных нейронных сетей (например, для распознавания изображений — сверточных), адаптированной к реализации на малогабаритных вычислителях отечественного производства, предназначенных для работы в экстремальных условиях. В качестве базовой архитектуры можно использовать отечественную разработку — NeuroMatrix. Благодаря ряду аппаратных особенностей микропроцессоры данной архитектуры могут быть использованы для работы с нейронными сетями.

В целом развитие автоматизированных и автоматических систем управления и обработки данных на основе технологий машинного обучения в области БПЛА является перспективным направлением повышения эффективности их применения в различных сферах деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Чуднов А. М., Губская О. А., Кичко Я. В. Методика анализа вероятностно-временных характеристик обмена сообщениями в комплексе беспилотных летательных аппаратов // Известия Тульского государственного университета. Технические науки. 2021. № 11. С. 117-124.
2. Сураев И. На «Армии-2019» показали систему управления стаей беспилотников // РИА Новости [Электронный ресурс] URL:https://ria.ru/20190628/1556017875.html (Дата обращения 09.06.2023).
3. Паращук И. Б., Михайличенко Н. В. Эффективность современных центров обработки данных // Перспективные направления развития отечественных информационных технологий. Материалы III межрегиональной научно-практической конференции : сборник / научный редактор Б. В. Соколов. 2017. С. 24-26.
4. В России впервые показали ударный беспилотник «Охотник» с плоским соплом // Информационное агентство ТАСС [Электронный ресурс] URL:https://tass.ru/armiya-i-opk/13191513 (Дата обращения 09.06.2023).

УДК 621.391.3

УЯЗВИМОСТИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ

Апарина Елена Юрьевна, Ащеулов Сергей Викторович,
Бабич Борис Иванович, Майер Софья Александровна
Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: elenaaparina.1982@mail.ru, asheulov50@mail.ru, babichbi@mail.ru, maysofa28@gmail.com

Аннотация. В статье приведены основные принципы работы программно-конфигурируемых сетей, рассмотрены основные угрозы информационной безопасности.

Ключевые слова: программно-конфигурируемая сеть, уязвимость, информационная безопасность.

VULNERABILITIES OF SOFTWARE-DEFINED NETWORKS

Aparina Elena, Ascheulov Sergey, Babich Boris, Maier Sofia
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av., St. Peterburg, 194064, Russia
e-mails: elenaaparina.1982@mail.ru, asheulov50@mail.ru, babichbi@mail.ru, maysofa28@gmail.com

Abstract. The article presents the basic principles of operation of software-defined networks, discusses the main threats to information security.

Keywords: Software-defined network, vulnerability, information security.

В существующих системах обмена данными неизбежно растет поток разнообразной информации, которую необходимо своевременно собирать, надлежащим образом обрабатывать и оперативно использовать по назначению. Кроме того, современные потребности пользователей в своевременном, достоверном и безопасном предоставлении новых сетевых услуг, опережают технические возможности провайдеров для их реализации. Решение данного противоречия сегодня видится в использовании новых телекоммуникационных технологий, таких как программно-конфигурируемые сети (от англ. *Software-defined Networking SDN)*, также программно-определяемая сеть — сеть передачи данных, в которой уровень управления сетью отделён от устройств передачи данных и реализуется программно, одна из форм виртуализации вычислительных ресурсов.

К основным свойствам *SDN* следует отнести [1, 2]:

– разделение плоскостей управления и передачи данных;

– виртуализация сетевых функций *NFV (Network Functions Virtualization)*;

– программируемое управление сетевыми ресурсами, вычислительными ресурсами и ресурсами хранения данных, а также оркестрацией — управление жизненным циклом услуг;

– стандартизация протоколов и автоматизация конфигурации сетевых элементов;

– единый механизм администрирования и выделения ресурсов сети по запросу для различных услуг и функций;

– автоматизация управления, развертывания сетевых элементов и бизнес-процессов [2-4].

Комплексное использование этих новых свойств позволяет реализовать динамическую подстройку сет и под нужды приложений, что повышает операционную гибкость и упрощает развёртывание услуг. Основная идея *SDN* состоит в том, чтобы, не изменяя существующего сетевого оборудования, отделить управление этим оборудованием (маршрутизаторами и коммутаторами) за счет создания специального программного обеспечения, которое может работать на обычном отдельном компьютере, находящемся под контролем администратора сети (контроллере). Для реализации этой идеи создан открытый протокол *OpenFlow* для управления маршрутизацией и коммутацией в сети. С помощью этого протокола специалисты сами могут определять и контролировать: кто с кем, при каких условиях и с каким качеством может взаимодействовать в сети. Все маршрутизаторы и коммутаторы объединяются под управлением сетевой операционной системы, которая обеспечивает приложениям доступ к управлению сетью и постоянно отслеживает конфигурацию средств сети [1-3].

Преимущества *SDN*. Централизация управления. Что позволяет упрощать процесс определения оптимального маршрута и только потом вносить изменения в таблицу потоков коммутатора, а также производить все сложные вычисления в контроллере, а вместо дорогостоящих маршрутизаторов использовать более простые устройств.

Масштабируемость. Имея возможность *SDN* выделять ресурсы по своему усмотрению, возможно изменить сетевую инфраструктуру в любой момент. Это достигается за счет того, что приложения могут работать на нескольких системах одновременно. Масштабирование в концепции *SDN* представляет собой просто добавление новых физических систем, а не наращивание мощности существующей.

Увеличение возможностей для модернизации сети, т.к. модернизация сети *SDN* — это задача написания нового приложения. Развертывание *SDN* позволяет администратору оптимизировать использование оборудования и работать более эффективно за счет его виртуализации.

К недостаткам архитектуры *SDN* можно отнести следующие. Единая точка отказа. В случае выхода из строя контроллера, ко всем коммутаторам будет применена базовая конфигурация по умолчанию, и весь функционал, ранее установленный контроллером, будет утерян. А также критичность к ошибкам в настройке контроллера, которые в итоге могут привести к отказу всей сети [1, 3, 4].

Отдельно необходимо рассмотреть потенциальные уязвимости архитектуры *SDN* с точки зрения информационной безопасности. При проектировании *SDN*-сетей необходимо принимать во внимание следующие аспекты безопасности: разделение доступа сетевых приложений при работе с контроллером, вопросы аутентификации и авторизации при работе приложений с контроллером, а также, наряду с надежной аутентификацией всех ролей участников сети, необходимо предусмотреть шифрование данных о пользователях с возможностью контроля со стороны пользователя. [3, 5, 6].

Контроллер как ключевой компонент в управлении всей инфраструктурой *SDN* является наиболее уязвимым элементом, атака на который может повлечь критичные для всей инфраструктуры последствия. Разделение доступа сетевых приложений в соответствии с характером выполняемой задачи должны быть детально описаны. С этой целью применяются различные модели разграничения доступа (ролевые, мандатные, дискреционные и их комбинации).

Режимы работы контроллера (реактивный или проактивный) могут быть легко идентифицированы злоумышленником без применения специфичных подходов и программного обеспечения. В результате некоторые атаки могут использовать конкретный режим работы контроллера. Так, несанкционированная установка правил обработки на коммутаторах, которая приводит к снижению эффективности или нарушению работы сети, проще реализуется в реактивном режиме.

Угрозы безопасности, актуальные для большинства информационных систем, такие как сканирование портов и определение сетевых служб, являются критическими для архитектуры *SDN* по причине уязвимости канала *OpenFlow* и наличия большого количества трафика управления, передаваемого между коммутаторами и сетевыми контроллерами (также могут являться предшественниками направленных *DoS*-атак).

Одним из самых опасных для архитектуры *SDN* с централизованной точной управления — *DoS*-атаки «отказ в обслуживании». Так как передающие устройства не имеют функций управления, они должны иметь стабильное подключение к сетевому контроллеру, чтобы обеспечивать передачу данных. В реактивном режиме контроллера даже короткий период недоступности может вызвать много проблем для сетевой инфраструктуры, а долгосрочное блокирование полностью остановит обработку сетевого трафика. К тому же такая ситуация позволит провести более сложную атаку. Например, ложный сетевой контроллер может занять место заблокированного, что ставит под угрозу всю сетевую инфраструктуру.

Другой потенциальной проблемой является уязвимость программной инфраструктуры *SDN*. Возможность программирования сети и наличие открытых программных интерфейсов, используемых для интеграции с сетевым контроллером, открывают возможность для появления уязвимостей программного обеспечения.

Еще одна угроза, характерная для традиционной сетевой инфраструктуры — атака с подменой — имеет более высокий потенциал для сетей *SDN*, чем в традиционных сетях. В то время как вся сеть управляется централизованным контроллером, риск подмены трафика управления в сети *OpenFlow* достаточно высок. Причина этому — организация взаимодействия между сетевым контроллером и коммутаторами на базе протокола *TCP* без шифрования, а поддержка протокола *TLS* является необязательной. Подмена может повлечь несанкционированный доступ к сетевым устройствам, получение контроллером некорректной статистики или данных о состоянии сети, что может сказаться на работе всей сети.

Основными угрозами, возникающими со стороны сетевых устройств, работающих по принципу программно-конфигурируемой сети, остаются вариации таких атак, как *DoS*, подмена контроллера и т.д. Наиболее простым и одновременно эффективным способом нарушения целостности работы сети *SDN* являются атаки типа *DoS*. Опасность атаки следует из самого алгоритма работы *SDN*-коммутатора при получении неизвестного пакета. Последствия данной атаки: расход процессорных ресурсов коммутатора при пересылке контроллеру неизвестных пакетов; перегрузка канала связи между коммутатором и контроллером «пустыми» данными и невозможность доставки управляющих сообщений; перегрузка контроллера приходящими запросами и невозможность обработки управляющих сообщений, вызванных легитимным трафиком.

Стоит отметить, что рассмотренные уязвимости, присущие архитектуре *SDN*, не отменяют угроз, связанных с традиционными сетями передачи данных, которые также являются критичными в той же или большей степени для сетей *SDN*. Однако, централизация управления, доступная не только сетевому контроллеру,

но и интегрированным с ним приложениям в архитектуре *SDN*, предоставляет возможность, как усовершенствовать имеющиеся, так и создавать принципиально новые средства защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. Докучаев В. А., Иевлев О. П., Маклачкова В. В., Шалагинов А. В. Программно-конфигурируемая архитектура приложений и инфраструктуры. М., 2020. С. 4-7.
2. Сетевые технологии SDN — Software Defined Networking [Электронный ресурс]. URL: https://habr.com/ru/companies/muk/articles/251959/ (дата обращения: 30.06.2023).
3. Бахарева Н. Ф., Ушаков Ю. А., Ушакова М. В., Шухман А. Е. Основы программно-конфигурируемых сетей. Самара : Поволжский государственный университет телекоммуникаций и информатики, 2015. С. 30-32.
4. Ошкина Е. В. Сетевая технология SDN (обзор, современные тенденции) // Технические науки: проблемы и перспективы : материалы V Междунар. науч. конф. (Санкт-Петербург, июль 2017 г.). Санкт-Петербург : Свое издательство, 2017. С. 3-6. [Электронный ресурс]. URL: https://moluch.ru/conf/tech/archive/231/12628/ (дата обращения: 30.06.2023).
5. Пархомик С. Ю., Семак А. Д., Селезнев И. Л. Автоматизация и масштабирование локальных вычислительных сетей с использованием SDN // Международный научно-тезнический семинар, 2017. С. 57-63 [Электронный ресурс]. URL: https://libeldoc.bsuir.by/bitstream/123456789/30132/1/Parkhomik_Avtomatizatsiya.PDF (дата обращения: 30.06.2023).
6. Захаров А. А., Попов Е. Ф., Фучко М. М. Аспекты информационной безопасности архитектуры SDN // Вестник СибГУТИ. 2016. № 1. С. 83-92.

УДК 621.391.3

ЗАЩИТА СЕТЕВЫХ УСТРОЙСТВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Апарина Елена Юрьевна, Ащеулов Сергей Викторович,
Бабич Борис Иванович, Патов Григорий Владиславович
Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: elenaaparina.1982@mail.ru, babichbi@mail.ru, asheulov50@mail.ru, grisha.patov@mail.ru

Аннотация. В статье рассматриваются основные функции уровней модели взаимодействия открытых систем, а также совокупность основных протоколов, реализованных на каждом уровне и относящиеся к ним сетевые устройства. Рассмотрены механизмы обеспечения безопасности сетевых устройств, обеспечивающих защиту от несанкционированного доступа.

Ключевые слова: модель взаимодействия открытых систем, протокол, несанкционированный доступ.

PROTECTION OF NETWORK DEVICES FROM UNAUTHORIZED ACCESS

Aparina Elena, Babich Boris, Ascheulov Sergey, PatovGrigory
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails:toni09_91@mail.ru,shchuk@rambler.ru, andrsel@mail.ru

Abstract. The article discusses the main functions of the levels of the open systems interaction model, as well as a set of basic protocols implemented at each level and related network devices. The mechanisms of ensuring the security of network devices that provide protection against unauthorized access are considered.

Keywords: open systems interaction model, protocol, unauthorized access.

В связи с развитием электронно-вычислительной техники в течение последних 20-ти лет наряду с процессами обмена сообщениями между людьми (телефонными, телеграфными и т.п.) существенную роль стали играть процессы хранения и содержательной обработки информации, появились новые типы информационного взаимодействия. Компьютерные сети, обеспечивающие не только обмен информационными сообщениями, но и их обработку, доступ к базам данных, поиск, сбор, хранение информации и т.п., стали называть информационными сетями. Вместе с тем, сегодня часто используется понятие инфокоммуникационная сеть, которое более четко отображает тот факт, что в сети осуществляется как обработка информации, так и обмен информационными сообщениями между узлами сети и оконечным оборудованием пользователей.

В тоже время инфокоммуникационная сеть представляет собой эффективную, но вместе с тем и непредсказуемую среду, полную разнообразных угроз и опасностей. Большая группа угроз связана с несовершенством протоколов, в частности протоколов стека TCP/IP, которые разрабатывались в то время, когда проблема обеспечения информационной безопасности еще не стояла довольно остро.

Многообразие угроз породило многообразие методов защиты, к которым можно отнести основные технологии обеспечения информационной безопасности: аутентификацию и авторизацию, шифрование и антивирусные средства, сетевые экраны и прокси-серверы, защищенные каналы и виртуальные частные сети [1, 2].

Целью данной работы является анализ основных функции всех уровней модели *OSI*, а также реализованные протоколы и стандартные способы защиты от НСД на каждом уровне, на примере сети стека *TCP/IP*. [3, 4, 6] Рассматриваемые услуги защиты на каждом уровне *OSI* регламентированы в [4], в качестве механизмов защиты рассматриваются конкретные протоколы, реализующие услуги защиты [1-6].

Современные инфокоммуникационные сети и входящие в их состав телекоммуникационные сети представляют собой сложные иерархические системы, которые описываются с помощью понятия архитектура сети и характеризуются многоуровневым построением [1-3]. Чтобы систематизировать и урегулировать весь

перечень функций, которые должны быть выполнены, чтобы две машины (ЭВМ) могли взаимодействовать друг с другом, в начале 80-х годов международными организациями такими как: *ITU (International Telecommunications Union), ISO (International Standards Organization)* и другими была разработана эталонная модель взаимодействия открытых систем *OSI (Open System Interconnection)* [4]. Она предназначена для обобщенного представления функций средств сетевого взаимодействия и определяет уровни взаимодействия, стандартные названия уровней и функции, которые должны выполняться на каждом уровне.

В модели OSI определено семь уровней, причем нумерация начинается с нижнего:

7. Прикладной уровень (*application layer*);
6. Представительский уровень или уровень представления (*presentation layer*);
5. Сеансовый уровень (*session layer*);
4. Транспортный уровень (*transport layer*);
3. Сетевой уровень (*network layer*);
2. Канальный уровень (*datalink layer*);
1. Физический уровень (*physical layer*).

Протоколы седьмого-четвертого уровней определяют правила взаимодействия между удаленными объектами (т. е. из конца в конец), а протоколы третьего-первого уровней — правила взаимодействия соседних объектов сети, например, узлов.

Иерархическая структура стека *TCP/IP* предполагает объединение нижних двух уровней в один — уровень сетевых интерфейсов, а прикладной уровень стека *TCP/IP*, соответствует верхним трем уровням модели *OSI*: сеансовому, представления и прикладному [1, 5].

Физический уровень имеет дело с передачей потока данных (бит) по физическим каналам связи от одного узла к другому в виде электрического сигнала. Он определяет электрические и механические характеристики подключения к физическим каналам различного типа (телефонный канал, физическая линия, спутниковый канал и т.д.) Технологии физического уровня: технологии проводного абонентского доступа *x DSL (digital subscriber line); SDH (Synchronous Digital Hierarchy); PDH (Plesiochronous Digital Hierarchy); V.21-V.42* (протоколы модемной связи), технологии спектрального (волнового) мультиплексирования (*WDM Wavelength Division Multiplexing*) и другие.

В качестве оборудования, реализующего функции физического уровня применяются: мультиплексоры (*PDH, SDH, WDM*), модемы *xDSL*, радиомодемы, концентраторы (*Ethernet*), повторители, регенераторы, и т. п.

Единица данных — бит.

Услуги защиты: конфиденциальность в режиме с установлением соединения, конфиденциальность потока трафика [4].

Механизм защиты — полное шифрование потока данных с помощью устройств шифрования.

Канальный уровень обеспечивает доставку пакетов между любыми узлами пакетной сети, построенной с использованием определенной технологии канального уровня *(Eternet, Frame Relay, Wi-Fi, FDDI* и т.п.)

Канальный уровень разделен на два подуровня: *LLC (Logical Link Control)* —- управление логическим каналом и *MAC (Media Access Control)* — управление доступом к среде.

Уровень *LLC* единый для всех стандартов, представляет собой обобщение функций разных технологий по обеспечению передачи кадра с различными требованиями к надежности. Функции уровня *MAC*– обеспечение доступа к разделяемой среде; передача кадров между конечными узлами посредством функций и устройств физического уровня. Каждой технологии *MAC*-уровня соответствует несколько спецификаций протоколов физического уровня. Так, стандарт *FastEthernet* (802.3*u*) установил три спецификации:*100Base-T4*; *100Base-TX*; *100Base-FX*.

В качестве оборудования, реализующего функции канального уровня применяются коммутаторы и мосты, также он реализован в модемах, маршрутизаторах, компьютерах [1]. Единица данных — кадр.

На канальном уровне также работают и другие протоколы, решающие дополнительные задачи:

PPP (Point-to-Point Protocol) — позволяет передавать через модемное соединение точка-точка любой сетевой трафик путем использования инкапсуляции;

STP (SpanningTreeProtocol) устраняет петли в топологии сети *Ethernet, ARP (AddressResolutionProtocol)* предназначен для определения *MAC*-адреса по известному *IP*-адресу;

MPLS (MultiProtocol Label Switching) — объединяет технику виртуальных каналов с функциональностью стека *TCP/IP* (передача данных с помощью меток) и другие [1-3].

Услуги защиты: конфиденциальность в режиме установления соединения, конфиденциальность в режиме без установления соединения [4].

Механизмы защиты:

– шифрование данных до этапа выполнения основных функций канального уровня;
– создание виртуальных локальных сетей *VLAN (Virtual Local Area Network*), позволяющих сегментировать трафик в локальной вычислительной сети (ЛВС);
– применение технологии защищенного канала с помощью системных средств — протокол *PPP;*
– парольная защита сетевых устройств.

Сетевой уровень — служит для образования единой транспортной системы, объединяющей разнородные сети, называемой составной сетью, или интернетом. Основная задача данного уровня определить маршрут и

доставить сетевые пакеты узлу получателю вне зависимости от его местонахождения. На данном уровне работают такие протоколы, как:

IPv4 (IPv6) (Internet Protocol) сетевой протокол объединяет сегменты сети в единую сеть, обеспечивая доставку пакетов данных между любыми узлами объединенной сети;

RIP (Routing Information Protoco), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol) и другие протоколы маршрутизации, позволяющие строить карту сети и определять маршруты передачи;

ICMP (Internet Control Message Protocol) протокол межсетевых управляющих сообщений, передающий сообщения об ошибках и других исключительных ситуациях, возникающих при передаче;

VRRP (Virtual Router Redundancy Protocol) — позволяет объединять несколько физических маршрутизаторов в один виртуальный, и другие протоколы, решающие частные задачи на сетевом уровне.

Устройства сетевого уровня — маршрутизаторы, также сетевой уровень реализован на компьютерах, также возможны коммутаторы третьего уровня. Единица данных — пакет.

Услуги защиты:

– аутентификация равноправного логического объекта, также отправителя;
– управление доступом;
– конфиденциальность в режиме с/без установления соединения;
– конфиденциальность потока трафика;
– целостность в режиме с/без установления соединения [4].
– Механизмы защиты:
– управление доступом к сетевым устройствам (использование средств аутентификации, авторизации и учета пользователей);
– межсетевое экранирование, использование стандартных списков контроля доступа *ACL (Access Control List)* сцелью фильтрации сетевых пакетов;
– обеспечения безопасности на основе виртуальных частных сетей с шифрованием трафика, протокол *IPSecurity*;
– применение технологии *NAT (Network Address Translator),* которая позволяет не только экономить публичные *IP*-адреса, но и скрывать адресную структуру ЛВС и др.

Следующим уровнем является транспортный. В отличие от первых трех, задачей которых является доставка данных до узла сети, транспортный доставляет данные непосредственно до приложений, ведущих сеанс на ЭВМ. Кроме того, этот уровень предоставляет передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет 5 классов транспортного сервиса от низшего класса 0 до высшего класса 4. Эти виды сервиса отличаются качеством предоставляемых услуг. Благодаря протоколам транспортного уровня одновременно работающих приложений может быть несколько. Протоколы успешно будут разделять потоки данных к каждому из них. Идентификация процесса получателя осуществляется по расширенному адресу, состоящему из двух частей: *IP*-адреса, идентифицирующего оконечное устройство, и номера порта, идентифицирующего прикладной процесс.

Транспортный уровень реализован на оконечных устройствах — компьютерах. Основные протоколы транспортного уровня стека *TCP/IP*:

TCP (Transmission Control Protocol) — протокол управления передачей. Обеспечивает гарантированную доставку сообщений в режиме с установлением соединения. Протокольный блок данных *TCP* называется сегментом;

UDP (User Datagram Protocol) — дейтаграммный протокол пользователя. Не обеспечивает гарантированную доставку сообщений, а осуществляет ее «по возможности» без установления соединения и другие. Протокольный блок данных — дейтаграмма.

Услуги защиты:

– аутентификация равноправного логического объекта, также отправителя;
– управление доступом;
– конфиденциальность в режиме с/без установления соединения;
– конфиденциальность потока трафика;
– целостность в режиме с установлением соединения с/без восстановлением;
– целостность в режиме без установления соединения.

Механизмы защиты:

– на этом уровне может выполняться шифрование и дешифрование данных, благодаря которым секретность обмена данными обеспечивается сразу для всех прикладных служб. Применяются протоколы *SSL (Secure Socket Layer*) или *TLS (Transport Layer Security)*. Создается защищенный канал, используя следующие технологии безопасности: взаимная аутентификация приложений на обоих концах защищённого канала выполняется путем обмена сертификатами; для контроля целостности передаваемых данных используются дайджесты; секретность обеспечивается шифрованием с использованием симметричных ключей сеанса.
– включение процедуры аутентификации каждого *TCP*-сегмента с использованием цифровой подписи (цифровая подпись не обеспечивает конфиденциальности, содержимое защищаемых полей не шифруется, но она гарантирует, что *TCP*-сегмент не был изменен третьей стороной).

Сеансовый уровень управляет взаимодействием сторон и обеспечивает передачу данных в диалоговом режиме, а также предоставляет средства синхронизации сеанса. В отличие от нижестоящих уровней, выделенных

протоколов сеансового уровня не существует. Функции этого уровня интегрированы в протоколы, которые выполняют также функции уровней представления и прикладного [1, 4].

К протоколам, выполняющим функции сеансового уровня относят следующие:

SIP 2.0 (Session Initiation Protocol) — протокол инициирования сеанса. Представляет собой протокол для сигнализации и ответственен за установление сеанса между абонентами;

PPTP (Poit-to-Point Tunneling Protocol) — туннельный протокол типа точка-точка. Позволяет компьютеру устанавливать защищенное соединение с сервером за счет создания специального туннеля в стандартной, незащищённой сети;

L2TP (Layer 2 TunnelingProtocol) — протокол туннелирования второго уровня. Позволяет организовать *VPN* с заданными приоритетами доступа, однако не содержит в себе средств для защиты данных и механизмов аутентификации;

PAP (Password Authentication Protocol) — протокол аутентификации по паролю при передаче его по сети в открытом виде и другие.

На данном уровне не предусматривается никаких услуг защиты [4]. Однако протоколы туннелирования, относящиеся к сеансовому уровню, выполняют в том числе и функцию защиты соединения.

Уровень представления данных преобразует данные в соответствующий формат посредством кодирования и сжатия. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например, кодов *ASCII* и *EBCDIC*. К функциям уровня представления относится также кодирование графических изображений, аудио и видео в соответствии с различными стандартами, например, *JPEG, MPEG, TIFF*. Уровень представления данных реализован на ЭВМ, единица данных — файл.

Услуги защиты:

– конфиденциальность в режиме с/без установления соединения;
– конфиденциальность выбранных паролей.

Механизм защиты — протокол безопасности транспортного уровня *TLS*, который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека *TCP/IP*, заменивший протокол защищенных сокетов *SSL* в виду его неблагонадежности;

Механизмы защиты уровня представления могут использоваться совместно с механизмами прикладного уровня. Прикладной уровень — осуществляет связь пользовательских приложений с сетью. Для запросов к прикладному уровню используются системные вызовы операционной системы, образующие прикладной программный интерфейс, например:

DHCP(Dynamic Host Configuration Protocol) — протокол динамического конфигурирования хостов.

HTTP(Hyper Text Transfer Protocol) — протокол передачи гипертекста.

SMTP(Simple Mail Transfer Protocol), POP 3 (Post Office Protocol), IMAP (Internet Mail Access Protoco) — протоколы, используемые системой электроной почты;

FTP (File Transfer Protocol) — протокол передачи файлов.

TELNET(Telecommunication Network) обеспечивает эмуляцию алфавитно-цифрового терминала, (удаленное управление);

SNMP(Simple Network Management Protocol) — простой протокол управления сетью и другие

Реализован на ЭВМ, единица данных — файл.

Услуги защиты:

– аутентификация равноправного логического объекта, также отправителя;
– управление доступом;
– конфиденциальность в режиме с/без установления соединения;
– конфиденциальность потока трафика;
– целостность в режиме с/без установления соединения.

Механизмы защиты:

– реализация защищенного канала на прикладном уровне, хотя протокол защищает только определенную сетевую службу, например, файловую, гипертекстовую или почтовую. Так, протокол *S/MIME* защищает сообщения электронной почты. При таком подходе для каждой службы необходимо разрабатывать собственную защищенную версию протокола. Протокол защищенного канала на уровне представления делает его более универсальным средством [1];

– использование в качестве протокола удаленного доступа протокола *SSH (Secure SHell*), т. к. данные в *TELNET* передаются в незашифрованном виде;

– аналогично, рекомендуется выбирать следующие защищенные сетевые протоколы: *SFTP* вместо *FTP, SCP* вместо *TFTP, SNMPv3* вместо *SNMPv1* и *SNMPv2* [6].

Таким образом, анализ ряда работ показал, что при большом многообразии протоколов защиты данных от НСД сетей *TCP/IP* используются три основных подхода: защита с помощью протоколов данного уровня; защита совместно с протоколами других уровней; защита с использованием механизмов нижестоящих уровней.

СПИСОК ЛИТЕРАТУРЫ

1. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: юбилейное издание. СПб.: Питер, 2020. 1008 с. (Учебник для вузов).
2. Галас В. П. Сети и телекоммуникации. Часть 2 // Вычислительные системы, сети и телекоммуникации : учебник : в 2 ч. Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. Владимир : Изд-во ВлГУ, 2017. 284 с. ISBN 978-5-9984-0817-5 (ч. 2). ISBN 978-5-9984-0731-4.

3. Инфокоммуникационные системы специального назначения : учеб. пособие / под ред. С. М. Одоевского. СПб.: ВАС, 2016. 447 с.
4. ГОСТ Р ИСО 7498-2-99. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. М.: ИПК Издательство стандартов, 1999.
5. ISO/IEC 7498-1:1994 Information technology — Open Systems Interconnection — Basic reference model: The basic model (Информационные технологии. Взаимосвязь открытых систем. Базовая эталонная модель: Базовая модель). М., 1999. 59 с.
6. Безопасность компьютерных сетей : учеб. пособие / А. С. Коноплев [и д.р.]. СПб.: ПОЛИТЕХ-ПРЕСС, 2022. 90 с.

УДК 004.0056

ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ОБРАБОТКИ ИНФОРМАЦИИ

Ащеулов Сергей Викторович, Михайличенко Николай Валерьевич,
Грибков Владимир Александрович, Мишутин Никита Вячеславович
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: 23esn2008@rambler.ru

Аннотация. В настоящее время, вопросы построения центров обработки данных возросли во всем мире. Центры обработки данных (ЦОД) или как их стало принято называть дата-центры — это высоконадежная система, обеспечивающая автоматизацию процессов с высоким уровнем производительности и качеством предоставляемых сервисов. Информация, которая обрабатывается дата-центрами растет с каждым годом, так же, как и ее ценность. Вместе с данными наблюдается быстрое развитие видов связи и услуг: электронной и голосовой почты, IP телефонии, сервисов мгновенного обмена сообщениями, видеоконференций и т.п. Таким образом, можно отметить, что с ростом объемов информации, растет и число приложений, а, следовательно, возникает необходимость в централизованной системе обработки и хранения информации. Именно поэтому владельцы дата-центров заинтересованы в постоянном увеличении их числа и снабжении дата-центров самым современным, технологичным и качественным оборудованием.

Ключевые слова: центры обработки данных; дата-центры; автоматизированная система обработки информации.

DATA PROCESSING CENTERS IN AUTOMATED INFORMATION PROCESSING SYSTEM

Asheulov Sergey, Mihaylichenko Nikolay, Gribkov Vladimir, Mishutin Nikita
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: 23esn2008@rambler.ru

Abstract. Currently, the issues of building data centers have increased all over the world. Data processing centers (data centers), or as they have become commonly called data centers, is a highly reliable system that provides automation of processes with a high level of productivity and quality of services provided. The information that is processed by data centers is growing every year, as well as its value. Along with the data, there is a rapid development of types of communication and services: e-mail and voice mail, IP telephony, instant messaging services, video conferencing, etc. Thus, it can be noted that with the increase in the volume of information, the number of applications is also growing, and therefore there is a need for a centralized system for processing and storing information. That is why the owners of data centers are interested in constantly increasing their number and supplying data centers with the most modern, technological and high-quality equipment.

Keywords: data processing centers; data centers; automated information processing system.

На сегодняшний день новейшая IT-инфраструктура является неотъемлемой частью жизни как крупных корпораций, так и совсем небольших предприятий. Такая ситуация призывает к неизбежному совершенствованию системы управления специальными силами и средствами. Вопросы непрерывного функционирования информационных систем остро встают в современных условиях их функционирования, появляются проблемы увеличения объема и ценности информации в процессе выхода из строя систем такого класса. Одним из базовых элементов построения современной IT-инфраструктуры являются центры обработки данных (ЦОД) [1].

Дата-центр выполняет функции обработки, хранения и передачи информации, как правило, в интересах корпоративных клиентов — он ориентирован на решение задач путём предоставления информационных услуг. Консолидация вычислительных ресурсов и средств хранения данных в ЦОД позволяет сократить совокупную стоимость владения IT-инфраструктурой за счёт возможности эффективного использования технических средств, например, перераспределения нагрузок, а также за счёт сокращения расходов на администрирование.

Центры обработки данных обычно расположены в пределах или в непосредственной близости от узла связи или точки присутствия какого-либо одного или нескольких операторов связи. Качество и пропускная способность каналов влияют на уровень предоставляемых услуг, поскольку основным критерием оценки качества работы любого дата-центра является время доступности сервера.

В основном ЦОД необходим крупным компаниям, использующим мощные информационные системы, и где информация напрямую влияет на выполнение основных процессов. К таким компаниям можно отнести:

телекоммуникации (операторы услуг связи); финансовый сектор (банки, брокеры); страховые компании; транспортные компании; государственные структуры; другие крупные компании.

Помимо крупных компаний, дата-центры могут быть интересны из-за необходимости в обеспечении отказоустойчивой, надежной системы хранения данных.

К преимуществам ЦОД можно отнести [2]:

– отказоустойчивость и надежность системы;
– высокий уровень защиты информации;
– возможность оптимизации процессов;
– централизованное управление и улучшение контроля;
– гибкость и масштабируемость системы;
– снижение стоимости эксплуатации IT-структуры.

К современным ЦОД предъявляется ряд общих требований [3]:

– должен предоставлять возможности эффективного взаимодействия сетевых сервисов предприятия;
– должен предоставить возможность гибкого масштабирования информационной системы;
– должна быть реализована отказоустойчивость на уровне выхода из строя любого коммутационного узла или канала связи ЦОД;
– должна быть реализована отказоустойчивость на уровне выхода из строя одного накопителя данных в любом узле;
– должен иметь надежную систему резервного копирования информационных баз предприятия;
– при использовании системы резервного копирования риски фатального исхода должны быть минимизированы;
– оборудование ЦОД должно обеспечиваться постоянной подачей электропитания в случаях его аварийного отключения;
– для индивидуальных пользователей или групп пользователей должна быть возможность установки различных уровней доступа к процессам функционирования.

Важной составляющей инженерной инфраструктуры ЦОД является система подводки оборудования, с которой начинается проектирование. От настроек, заложенных на этапе проектирования в дальнейшем, будут определяться такие параметры как: надежность (отказоустойчивость), стоимость и управляемость будущего центра обработки данных.

В ходе проектирования центра обработки данных определяются параметры требуемой энергетической мощности и параметры теплообмена, это самые важные и необходимые для стабильной работы параметры. Также оговаривается предполагаемый срок службы центра.

На этапе проектирования должны быть указаны возможные ограничения существующих инженерных систем, прежде всего кондиционирования воздуха, необходимость выделения достаточных площадей для установки вспомогательных инженерных систем, таких как чиллерные установки, баки-аккумуляторы холодоносителя и пр.

После того, как заказчик определился с составом размещаемого оборудования, на эскизе прорисовывается будущая схема размещения оборудования. Стандартом для ЦОД является применение 19-и дюймовых шкафов для установки серверов и сетевого оборудования.

По классической схеме эти шкафы устанавливаются таким образом, чтобы между ними образовывались «горячие» и «холодные» коридоры. В «холодные» коридоры подается воздух от кондиционеров, из «горячих» коридоров воздух забирается системой кондиционирования.

Кроме этой схемы очень часто применяются:

– модернизированные схемы с изоляцией «холодного» или «горячего» коридоров;
– закрытые системы кондиционирования, когда тепловые потоки «запираются» в объеме шкафа с оборудованием;
– системы с вытяжкой горячего воздуха из шкафа, внутрирядное кондиционирование и т.д.

Коммуникационный шкаф должен выдерживать вес установленного оборудования, который может достигать 1000 кг. При этом он должен сохранять свою жесткость и устойчивость. Современные шкафы для ЦОД, как правило имеют перфорированные передние и задние двери. При этом неиспользуемая фасадная площадь должна быть закрыта специальными заглушками.

Помещение необходимо оборудовать кабельными лотками, как для прокладки электрического кабеля, так и для кабелей связи. При проектировании необходимо учитывать их взаимное влияние и расположение будущей системы кондиционирования воздуха. Помещение должно комплектоваться комплексно. В этом случае при эксплуатации не возникнет проблем с доступом к какому-либо оборудованию, не будет проблем с заменой или модернизацией оборудования и расширением ЦОД.

Все параметры должны быть согласованы друг с другом, чтобы принятые решения максимально отвечали целям и задачам создания инженерной системы ЦОД.

СПИСОК ЛИТЕРАТУРЫ

1. TIA/EIA-942. Telecommunications Infrastructure Standard for Data Center (Телекоммуникационная инфраструктура для Центров Обработки Данных) Стандарт ANSI. // Программируя Вселенную. Квантовый компьютер и будущее науки / Сет Ллойд, 2019.
2. Лисецкий Ю. М. Построение современного территориально-распределенного центра обработки данных // Программные продукты и системы. № 2, 2008. С. 14-16.
3. Паращук И. Б., Михайличенко Н. В. Эффективность современных центров обработки данных // Материалы III-й Межрегиональной НПК Перспективные направления развития отечественных информационных технологий. Севастополь : СевГУ, 2017. С. 24-26.

УДК 004.7

ИМИТАЦИОННАЯ МОДЕЛЬ МНОГОКАНАЛЬНОЙ ЭФИРНОЙ СРЕДЫ ПЕРЕДАЧИ ДАННЫХ

Верзун Наталья Аркадьевна[1], Колбанев Михаил Олегович[1],
Романова Анна Александровна[2]

[1] Санкт-Петербургский государственный университет аэрокосмического приборостроения
наб. канала Грибоедова, 30-32, лит. А, 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, anya-romanova-07@yandex.ru

Аннотация. Рассматривается имитационная модель многоканальной эфирной среды передачи данных, моделирующая процесс передачи сообщений через беспроводную сенсорную сеть интернета вещей.

Ключевые слова: имитационная модель; многоканальная среда передачи данных; вероятностно-временные характеристики.

SIMULATION MODEL OF MULTI-CHANNEL DATA TRANSMISSION MEDIUM

Verzun Natalia, Kolbanev Mikhail, Romanova Anna

[1] Saint Petersburg State University of Aerospace Instrumentation
emb. Canal Griboedova, 30-32, letter A, St. Petersburg, 191023, Russia
[2] Nizhny Novgorod State University of Engineering and Economics
st. Oktyabrskaya, 22a, Knyaginino, 606340, Russia
e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, anya-romanova-07@yandex.ru

Abstract. A simulation model of a multichannel over-the-air data transmission medium is considered, which simulates the process of transmitting messages through a wireless sensor network of the Internet of things.

Keywords: simulation model; multichannel data transmission medium; probabilistic-temporal characteristics.

На практике процессы информационного взаимодействия в интернете вещей могут не соответствовать в полной мере тем предположениям, которые легли в основу аналитического моделирования. Поэтому целесообразным при проектировании систем интернета вещей является использование методов имитационного моделирования с применением специализированных средств [1].

Одним из распространённых инструментов разработки имитационной модели является [2] AnyLogic. Он помогает специалистам разных областей получить детальное представление о системах и процессах и оптимизировать их [3].

В докладе описывается имитационная модель, за основу которой взята многоканальная система множественного доступа с синхронно-временным доступом к эфирной среде передачи [4]. Предполагаем, что многоканальная система передачи данных — это совокупность технических средств, обеспечивающих одновременную и независимую передачу однотипных или разнотипных сообщений от источников по N каналам, организованным в беспроводной физической среде распространения сигналов электросвязи. Моделируемая многоканальная система может быть представлена системой массового обслуживания вида $M/D/N$. При проведении имитационных экспериментов были рассмотрены случаи одно (N=1), двух (N=2) и пяти (N=5) канальной среды передачи.

Имитационная модель позволяет описать объекты информационного взаимодействия интернета вещей и может применяться для проведения разнообразных экспериментов в целях проектирования, анализа и оценки работы интернета вещей.

В частности, на разработанной модели проводились эксперименты позволившие рассчитать и построить графики зависимостей временных и вероятностных характеристик: среднего времени и вероятности своевременного обслуживания, информационной скорости реального времени в беспроводной сети интернета вещей и пр., от различных параметров исследуемой многоканальной системы множественного доступа (интенсивность передачи сообщений, число каналов и др.), а также оценить влияние этих параметров на качество передачи и производительность сети.

СПИСОК ЛИТЕРАТУРЫ

1. Носков И. И., Богатырев В. А., Сластихин И. А. Имитационная модель локальной компьютерной сети с агрегированием каналов и случайным методом доступа при резервировании передач // Научно-технический вестник информационных технологий, механики и оптики. 2018. № 18(6). С. 1047–1053.
2. AnyLogic: имитационное моделирование для бизнеса [Электронный ресурс]. URL: https://www.anylogic.ru/ (дата обращения: 19.06.2023).
3. Верзун Н. А., Колбанев М. О., Романова А. А. Имитационное моделирование информационного взаимодействия в кибертехнической системе / // Информационная безопасность регионов России (ИБРР-2021) : Материалы XII Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 27–29 ноября 2021 года. — С. 211-212.
4. Романова А. А. Имитационная модель информационного взаимодействия в интернете вещей // Известия СПбГЭТУ ЛЭТИ. 2022. № 8. С. 69-76.

УДК 004.716:004.056

МОНИТОРИНГ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЯ НА ОСНОВЕ ТЕХНОЛОГИИ ИНТЕРНЕТА ВЕЩЕЙ

Воробьев Андрей Игоревич, Андреева Екатерина Александровна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
e-mail: aivorobev@etu.ru, eaandreeva@etu.ru

Аннотация. В составе возможностей технологии Интернета вещей может быть применим контроллер состояния человека в условиях влияния внешних источников воздействия. Рассмотрен прототип системы с мониторингом состояния человека, состояния внешней среды, фиксацию состояния человека и выхода из диапазона безопасного состояния.

Ключевые слова: интернет вещей; безопасность пользователя; безопасность технологии интернета вещей; мониторинг параметров человека.

MONITORING OF INFORMATION AND PSYCHOLOGICAL SECURITY OF THE USER BASED ON THE INTERNET OF THINGS TECHNOLOGY

Vorobev Andrey, Andreeva Ekaterina
Saint Petersburg Electrotechnical University
5 Professora Popova St, St. Petersburg, 197022, Russia
e-mail: aivorobev@etu.ru

Abstract. As part of the capabilities of the Internet of Things technology, a human condition controller can be applied under the influence of external sources of influence. A prototype of a system with monitoring of the human condition, the state of the external environment, fixing the human condition and getting out of the safe state range is considered.

Keywords: Internet of things; user security; Internet of Things technology security; human parameters monitoring; Arduino Pro Mini.

Интенсивная профессиональная и функциональная деятельность человека, нацеленная на решение задач, поставленных перед человеком обстоятельствами, жизненными целями, личными профессиональными и творческими интересами, должна поддерживаться как минимум работоспособным состоянием человека, желательно жизненно активным и инициативным. В силу личной обязательности или вынужденности своей деятельности, человек способен терять объективную картину своего физического и физиологического состояния. При пиковых или затяжных периодах интенсивной или чрезмерной нагрузки состояние человека может выйти из безопасного или допустимого диапазона свойственного ему работоспособного состояния. Для таких случаев в составе возможностей технологии Интернета вещей может быть применим контроллер состояния человека по тому перечню параметров, которые будут либо традиционно рекомендуемые, либо для него специфичными по роду деятельности или физиологической предрасположенности. Была поставлена задача разработки прототипа устройства, работающего в режиме мониторинга текущего состояния человека с контролем, фиксацией и информированием его состояния; выявлением, фиксацией и информированием состояния отклонения из интервала допустимого состояния; фиксацией и информированием о состоянии в случаях влияния внешних источников воздействия чрезвычайного характера.

Предварительное аналитическое исследование было решено ограничить тремя составляющими наблюдения: набор контролируемых параметров состояния человека; набор инструментальных средств контроля состояния человека; перечень внешних факторов, принимаемых во внимание. Средства наблюдения обеспечивают мониторинг состояния человека. Логистическое решающее устройство сопровождает мониторинг и состояния человека, мониторинг состояния внешней среды, фиксацию допустимого состояния человека и выхода из диапазона разрешённого и безопасного состояния. Обзор используемого инструментария технологии Интернета вещей, который позволяет анализировать состояние человека в режиме реального времени, позволил разработать прототип системы на доступной открытой аппаратной платформе Arduino, собирающей данные с помощью датчиков считывания параметров, микроконтроллеров, аналитических модулей, с выходом на коммуникационные средства в удобном беспроводном формате технологии Интернета вещей.

В состав инструментария считывания параметров состояния человека входят датчики температуры DS18B20, датчики сердцебиения XD-58C, датчики пульса XD-58C, аналитическое устройство и Bluetooth модуль HC-05.

В состав датчиков внешней среды могут входить датчики широкого спектра газов MQ-2, датчики углекислого газа MQ-135, датчики угарного газа MQ-7, также связанные с аналитическим устройством и Bluetooth модулем HC-05.

Полупроводниковые датчики газоанализатора MQ-2 могут использоваться для характеристик состояния человека как газоанализаторы концентрации алкоголя в выдыхаемом воздухе и контроля никотиновой задымленности.

Концентрирующее устройство, основой которго является плата Arduino Pro Mini, соединено при помощи двух Bluetooth модулей HC-05 с модулем-анализатором и модулем мониторинга биологической активности. Для

удобства пользователя концентрирующее устройство собирает информацию, формализует и отсылает их по Bluetooth модулю на смартфон, где информация может быть представлена пользователю в удобном для него формате или сигнально в виде push-уведомления.

Программная реализация выполнена как программное обеспечение Android приложения, пересылающего статистику на web-сервер, написанный на языке программирования Python.

СПИСОК ЛИТЕРАТУРЫ

1. Грингард С. Интернет вещей. Будущее уже здесь. СПб: Альпина Паблишер, 2017. 188 с.
2. Блум Д. Изучаем Arduino. Инструменты и методы технического волшебства. BHV, 2015. 336 с.
3. Артемьев И. Е., Зараменских И. Е. Интернет вещей. Исследования и область применения. Инфра-М, 2017. 188 с.
4. Воробьев А. И., Мышевский Е. Г. Разработка системы безопасности на основе технологии интернета вещей // Евразийское Научное Объединение. 2018. Т. 1. № 10 (44). С. 53-55.
5. Воробьев А. И., Колбанёв А. М., Колбанёв М. О. Экологическая безопасность информационных технологий // Геополитика и безопасность. 2015. № 4 (32). С. 90–99.

УДК 004.056

ИССЛЕДОВАНИЕ РЕШЕНИЙ, ОБЕСПЕЧИВАЮЩИХ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ НА ОСНОВЕ ВИРТУАЛЬНЫХ СЕТЕЙ

Горбунов Константин Сергеевич[1], Пантюхин Олег Игоревич[2], Солодухин Борис Владимирович[2]

[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Большевиков пр., 22, корп.1, Санкт-Петербург, 193232, Россия

[2] Военная академия связи им. Маршала Советского Союза С. М. Буденного, Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: mr.gks94@mail.ru, p_oleg99@mail.ru, boris.soloduxin@yandex.ru

Аннотация. В докладе представлены результаты исследования решений, обеспечивающих безопасность информационных ресурсов на основе построения виртуальной частной инфраструктуры организаций. Установлены уровни построения виртуальной частной сети, выявлены возможные угрозы информационной безопасности и соответствующие способы защиты от их реализации. Определены минимальные требования к обеспечению информационной безопасности виртуальной частной сети.

Ключевые слова: информационная безопасность; виртуальная частная сеть; информационные потоки.

IMPLEMENTATION OF SOLUTIONS, ENSURING THE SECURITY OF INFORMATION RESOURCES BASED ON VIRTUAL NETWORKS

Gorbunov Konstantin[1], Pantyukhin Oleg[2], Solodukhin Boris[2]

[1] The Bonch-Bruevich Saint Petersburg State University of Telecommunications, 22 Bol'shevikov Av., k.1, St. Petersburg, 193232, Russia

[2] The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny, 3 Tikhoretsky Av., St. Petersburg, 194064, Russia

e-mails: mr.gks94@mail.ru, p_oleg99@mail.ru, boris.soloduxin@yandex.ru

Abstract. The report presents the results of a study of solutions that ensure the security of information resources based on the construction of a virtual private infrastructure of organizations. The levels of building a virtual private network have been established, possible threats to information security and appropriate ways of protecting against their implementation have been identified. The minimum requirements for ensuring the information security of a virtual private network are defined.

Keywords: information security; virtual private network; information flows.

Осуществление решений, обеспечивающих безопасность корпоративных информационных ресурсов, значительно повышает результативность всего процесса информатизации в организациях, обеспечивая целостность, достоверность и конфиденциальность дорогостоящей деловой информации, циркулирующей в локальных и глобальной информационных средах. Любая организация или структура, заинтересованная в сохранении конфиденциальности собственной информации, вынуждена вкладывать огромные средства в создание и обеспечение системы защиты. Для многих предприятий и организаций необходимость в защите критически важной информации стоит особенно остро. В соответствии с этим, вопросам защиты информационного взаимодействия уделяется особое внимание. Более того, с переходом на новые информационные технологии в области передачи информации, круг вопросов по информационной безопасности значительно расширяется.

Под информационной безопасностью понимают защищённость информации от незаконного ознакомления, преобразования и уничтожения, а также защищённость информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной: попытки проникновения злоумышленников, ошибки персонала, выход из строя программных и аппаратных средств и др. [1].

Одним из таких решений при межсетевом взаимодействии является технология виртуальных частных сетей. Суть её заключается в создании защищённых виртуальных каналов между конечными точками взаимодействия в сети. Эти каналы скрыты от других пользователей сети подложными IP-адресами, а информация, циркулирующая по ним, криптографически защищена. Применение данной технологии для защиты информационного взаимодействия внутри корпоративной компьютерной сети организации вполне целесообразно.

В настоящее время в организациях применяют наиболее актуальные и популярные средства защиты, такие как: антивирусные программы, межсетевые экраны, системы обнаружения вторжений IDS/IPS, а также виртуальные частные сети (VPN). Виртуальные частные сети используются организациями для соединения с удаленными сайтами, а также с другими организациями, они состоят из каналов связи, арендуемых у различных телефонных компаний и поставщиков услуг интернета [1-3].

VPN (англ. Virtual Private Network — виртуальная частная сеть) — логическая сеть, которая создается поверх другой сети, например, Internet. VPN может объединить, например, несколько офисов организации в единую сеть с применением для связи между ними неподконтрольных каналов. Между каждой парой «отправитель-получатель» устанавливается своеобразный туннель — безопасное логическое соединение.

Основные преимущества виртуальных частных сетей:

– информация сохраняется в секрете;
– удаленные сайты могут осуществлять обмен информацией незамедлительно;
– удаленные пользователи не ощущают себя изолированными от системы, к которой они осуществляют доступ.

Из недостатков частных сетей стоит отметить их высокую стоимость.

Для характеристики преимуществ виртуальных частных сетей можно отметить:

– трафик шифруется для обеспечения защиты от прослушивания;
– осуществляется аутентификация удаленного сайта;
– обеспечивается поддержка множества протоколов;
– соединение обеспечивает связь только между двумя конкретными абонентами.

Шифрование должно быть сложным, чтобы гарантировать конфиденциальность передаваемой информации на то время, пока она будет актуальна.

В виртуальных частных сетях обычно используются следующие типы протоколов: VPN PPTP, L2TP/Ipsec, IKEv2/IPSec, IPSec, SSTP, OpenVPN, SoftEther, WireGuard.

Внедрение одного из протоколов с устойчивым шифрованием значительно повышает коэффициент защищенности канала связи к прослушиванию трафика. Частная сеть предприятия либо сеть общего пользования с наличием VPN соединений с использованием функций уровней L2VPN или L3VPN повышают защищенность в случае передачи данных по схеме point-to-point либо по схеме VPLS (англ. Virtual Private LAN Service — сервис виртуальной частной сети) в случае передачи данных на несколько точек заказчика [4-6].

Также стоит рассмотреть возможные внутренние и внешние угрозы. Понимание того, каких угроз стоит опасаться, позволяет создать наиболее безопасную сеть, так как это помогает избежать слабых мест в обеспечении безопасности и внедрить наиболее эффективные в рамках данной задачи программные и аппаратные средства защиты. Внешние угрозы (атаки) по своему виду могут быть разделены на: Ddos атаки; вирусную атаку (в данном случае — направленную); замену данных (подмену, несанкционированное редактирование); атаки, направленные на выведение сети из строя; копирование данных (ключей, паролей); перехват пакетов данных и др.

Минимальные требования к обеспечению безопасности информационных потоков VPN [1, 7]:

1. Ограничение доступа в помещения центра обработки данных организации с использованием систем контроля доступа (противопожарные меры обеспечения безопасности, круглосуточное наблюдение).
2. Организация обработки критически важной (конфиденциальной) информации должна быть сегментирована от общих потоков данных.
3. Применение средств антивирусной защиты.
4. Должна быть установлена система обнаружения кибератак.
5. Доступ к базам данных хранилища информации и установление обновлений версий программного обеспечения должны фиксироваться в соответствующем журнале событий.
6. Аутентификация и идентификация должны реализовываться посредством алгоритмов шифрования, а также необходимо предусмотреть блокировку данных пользователя, не проходившего аутентификацию в течении трех месяцев.
7. Должны вестись журналы, в которых отражается информация об изменениях виртуальной инфраструктуры на платформах, развернутых посредствам системы виртуализации.
8. Хранение и обработка данных должна осуществляться в соответствии с требованиями законодательства Российской Федерации.

Информация, передаваемая посредствам технологий виртуализации, должна быть доступна только после аутентификации. Для этого используется взаимная аутентификация пользователя и серверов облака, которая должна быть построена на основе криптографии с открытым ключом (TLS, IPSec, AES).

Важным принципом в обеспечении безопасности VPN является необходимость использования единой политики безопасности для всех объединенных в VPN сетей, так как если хоть одна локальная вычислительная сеть, входящая в VPN, позволит осуществить незащищенный доступ, под угрозой будет находиться вся VPN.

Также необходимо учитывать, что VPN не обеспечивает защиту данных в конечных точках, это должно обеспечиваться посредствам криптографической защиты файлов, дисков, электронной почты, средствами защиты информации от несанкционированного доступа (должны быть идентичны средствам, установленным на VPN-устройствах), антивирусами.

СПИСОК ЛИТЕРАТУРЫ

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие. М.: ИД ФОРУМ : Инфра-М, 2010. 416 с.
2. Захватов М. Построение виртуальных частных сетей (VPN) на базе технологии MPLS. М.: Cisco Systems, 2001. 52 с.
3. Петренко С. Защищенная виртуальная частная сеть: современный взгляд на защиту конфиденциальных данных // Мир Internet. 2009. № 2. С. 15–17.
4. RFC 2637 Point-to-Point Tunneling Protocol (PPTP). The Internet Society, 1999.
5. RFC 2661 Layer Two Tunneling Protocol «L2TP». August, 2009.
6. RFC 8922 A Survey of the Interaction between Security Protocols and Transport Services.
7. Паращук И. Б., Саенко И. Б., Пантюхин О. И. Анализ состояния исследований по моделированию разграничения доступа к информации в облачных инфраструктурах критически важных информационных систем // Материалы седьмой Международная конференции НТиНМК. СПб : СПбГУТ, 2018. Т. 2. С. 524-529.

УДК 621.391 (075.8)

К ВОПРОСУ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕТИ

Ильина Ольга Борисовна[1], Купчиненко Ольга Павловна[1], Скоропад Александр Витальевич[2]
[1]Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
[2]Санкт-Петербургский филиал — «ЛОНИИР» (ФГБУ НИИР)
Большой Смоленский пр., 4, Санкт-Петербург, 192029, Россия
e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Аннотация. Рассмотрены задачи анализа сетевого трафика, особенности анализаторов трафика и их принцип работы. Сформулированы общие свойства и отличия снифферов. Проанализированы возможности консольных и графических утилит для мониторинга, анализа и визуализации сетевого трафика, которые могут помочь выявить проблемы в работе локальной сети.

Ключевые слова: анализ сетевого трафика; перехват пакетов; мониторинг трафика сети; сниффер; средства анализа сетевого трафика; безопасность сети.

ON THE ISSUE OF NETWORK SECURITY

Ilina Olga[1], Kupchinenko Olga[1], Skoropad Aleksandr[2]
[1]The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
[2]The M.I. Krivosheev Radio Research & Development Institute. LENINGRAD BRANCH — «LONIIR»
4 Bolshoy Smolensky Av, St. Petersburg, 192029, Russia
e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Abstract. The tasks of network traffic analysis, the features of traffic analyzers and their principle of operation are considered. The general properties and differences of sniffers are formulated. The possibilities of console and graphical utilities for monitoring, analyzing and visualizing network traffic, which can help identify problems in the operation of the local network, are analyzed.

Keywords: network traffic analysis; packet interception; network traffic monitoring; sniffer; network traffic analysis tools; network security.

Непрерывное совершенствование информационных и сетевых технологий, повышение их роли и значимости требуют постоянного внимания к вопросам обеспечения политики безопасности, без которой работоспособность сети может оказаться под угрозой. Анализ сетевого трафика в операционной системе специального назначения Astra Linux SE является одним из эффективных методов обеспечения безопасности сети. Актуальность анализа сетевого трафика растет в связи с развитием сетевых технологий, использованием новых сетевых протоколов и увеличением объема передаваемых по сети данных. Низкие требования, предъявляемые технологией анализа трафика сети к вычислительным ресурсам, позволяют анализировать большие объёмы сетевого трафика. Эта технология используется и для разграничения доступа извне к компьютерам и портам внутренней сети. На основе технологии анализа сетевого трафика разработаны сетевые списки контроля доступа ACL (Access Control List) на уровне IP-адресов и портов [1], а также на ее основе функционируют многие сетевые устройства: маршрутизаторы, большинство межсетевых экранов [2, 3] и другие устройства.

Анализ сетевого трафика — это метод, который с помощью захвата, записи и анализа трафика сети позволяет обнаруживать вредоносные программы, а также проблемы и ошибки различного типа, приводящие к замедленной или ненадежной работе сети. Анализ сетевого трафика используется для идентификации протоколов передачи данных, управления обменом данных и восстановления потоков данных в компьютерных сетях, а также для сбора статистики и решения задач мониторинга вычислительных сетей, который необходим и для предотвращения сетевых атак, и для выявления проблем в работе локальной сети.

Мониторинг трафика сети — это процесс непрерывного автоматизированного наблюдения за некоторыми параметрами трафика для проверки функционирования сети и предотвращения негативных событий (неисправных компонентов, а также атак и угроз безопасности).

Задачу анализа сетевого трафика можно разделить на независимые подзадачи: перехват, сохранение и анализ сетевых пакетов.

Анализ сетевого трафика позволяет изучить логику работы сети и перехватить поток данных, которыми обмениваются объекты сети.

Анализатор трафика или сниффер (sniffer) — это программное или аппаратно-программное устройство, работающее на канальном уровне модели OSI (Open Systems Interconnection) и предназначенное для мониторинга и анализа трафика сети.

Перехват трафика сети осуществляется с помощью режима «прослушивания» (promiscuous mode), который позволяет получать сетевые данные, предназначенные другим сетевым интерфейсам.

Снифферы могут перехватывать весь трафик и сохранять его в двоичном формате, а потом — расшифровывать. Они не используют правила протоколов верхнего уровня модели OSI [4] и обходят механизмы фильтрации, которые используются для интерпретации данных в стеке TCP/IP (Transmission Control Protocol / Internet Protocol).

Анализаторы трафика сети обладают следующими свойствами:

– измерения различных показателей трафика в сегменте локальной сети;
– работа с несколькими агентами, которые из разных сегментов локальной сети поставляют перехваченные пакеты;
– фильтрация отображаемых и перехваченных пакетов;
– использование условий начала и завершения процесса захвата сетевых данных;
– одновременная запись пакетов от нескольких сетевых адаптеров, позволяющая сопоставлять процессы, которые происходят в разных сегментах сети.

Различия сетевых анализаторов:

– возможность поддержки графического интерфейса;
– поддерживаемые сетевые протоколы;
– глубина анализа захваченных пакетов;
– возможность настройки фильтров до и после захвата сетевого трафика;
– совместимость с другими программами.

Сетевые анализаторы можно разделить на имеющие графический интерфейс и работающие из командной строки. Но, существуют снифферы и объединяющие эти возможности.

Некоторые анализаторы трафика сети могут захватывать и декодировать пакеты различных сетевых протоколов. Они распознают и поддерживают большое количество сетевых протоколов, могут их описать и декодировать по именам, а также определить, каким приложением порожден сетевой трафик.

Почти все сетевые анализаторы могут выполнять анализ декодированных пакетов. Графический интерфейс позволяет увидеть результаты декодирования пакетов с разной степенью детализации. Существуют снифферы с аналитическими модулями, которые позволяют создавать отчеты о перехваченном сетевом трафике.

Другой особенностью большинства анализаторов трафика является возможность настройки фильтров, как до захвата трафика сети, так и после него, что позволяет выделить из всего трафика пакеты, соответствующие заданным критериям и, таким образом, уменьшить объем перехваченной информации.

Некоторые снифферы обладают возможностью работать с перехваченным трафиком, сохраненным в файл своего формата или формата других сетевых анализаторов. Это позволяет провести более детальный анализ трафика сети.

Основной недостаток анализаторов трафика сети заключается в том, что они предоставляют большой объем сетевых данных, которые очень сложно анализировать.

С помощью средств анализа сетевого трафика можно создать инфраструктуру мониторинга сети. Например, используя планировщик заданий, можно в нужное время запустить сеанс сбора сетевого трафика, записать перехваченные сетевые данные в файл и с помощью сниффера проанализировать их.

Таким образом, снифферы представляют собой мощный инструмент диагностики сетевых проблем. Разные виды сетевых проблем, связанных с передачей и получением данных в сети, могут быть быстро определены и исправлены с помощью информации, полученной от анализатора сетевого трафика. Использование результатов анализа данных сетевого трафика позволяет оперативно найти и устранить неполадки, модернизировать компоненты сети и оптимизировать ее производительность. Для этого анализ данных выполняется как до, так и после изменений компонентов сети.

СПИСОК ЛИТЕРАТУРЫ

1. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 2. С 356-360.
2. Ильина О. Б., Купчиненко О. П., Скоропад А. В. К вопросу о сетевой безопасности и фильтрации пакетов // Актуальные проблемы инфокоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 2. С. 313-318.
3. Ильина О. Б., Купчиненко О. П., Скоропад А. В. К вопросу обеспечения информационной безопасности сети с помощью фильтрации пакетов // Информационная безопасность регионов России : материалы XI Санкт-Петербургской международной конференции, СПб, 23-25 октября 2019 г. СПб. : СПОИСУ, 2019. Т. 2. С. 434-436.
4. Деньжонков К. А. Основы построения и администрирования защищенной операционной системы специального назначения Astra Linux Special Edition : учебное пособие / К. А Деньжонков, А. В.Кий , В. В. Пащенко [и др.]. СПб : ВАС, 2019. 288 с.

УДК 621.391 (075.8)

УПРАВЛЕНИЕ ПРОГРАММНЫМИ ПАКЕТАМИ В СОВРЕМЕННОй ОПЕРАЦИОННОй СИСТЕМе СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Ильина Ольга Борисовна[1], Купчиненко Ольга Павловна[1], Скоропад Александр Витальевич[2]
[1]Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
[2]Санкт-Петербургский филиал — «ЛОНИИР» (ФГБУ НИИР),
Большой Смоленский пр., 4, Санкт-Петербург, 192029, Россия
e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Аннотация. Проведен анализ системы управления пакетами Advanced Packaging Tool в операционной системе специального назначения Astra Linux SE. Рассмотрены способы управления пакетами программ с помощью команд. Выполнено сравнение состава и назначения репозиториев в новых версиях операционной системе специального назначения Astra Linux SE Смоленск.

Ключевые слова: операционная система специального назначения; защита информации; пакет программ; система управления пакетами; репозиторий.

MANAGEMENT OF SOFTWARE PACKAGES IN A MODERN OPERATING SYSTEM OF SPECIAL PURPOSE

Ilina Olga[1], Kupchinenko Olga[1], Skoropad Aleksandr [2]
[1]The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
[2]The M.I. Krivosheev Radio Research & Development Institute. LENINGRAD BRANCH — «LONIIR»
4 Bolshoy Smolensky Av, St. Petersburg, 192029, Russia
e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Abstract. The analysis of the package management system Advanced Packaging Tool in operating systems of special purpose Astra Linux SE was done. Methods for managing software packages using commands are considered. Comparison of the composition and purpose of repositories in new versions operating systems of special purpose Astra Linux SE Smolensk is made.

Keyword: operating system of a special purpose; information security; software package; package management system; repository.

В современной операционной системе специального назначения (ОС СН) Astra Linux SE, дополнительное программное обеспечение (ПО) распространяется в виде пакетов (packages). В ОС СН Astra Linux SE, основанной на дистрибутиве Debian GNU Linux, используется система управления пакетами Advanced Packaging Tool (APT).

Система управления пакетами APT — это набор команд и дополнительных надстроек над ними (и графический интерфейс пользователя). Основной функцией APT является инсталляция, модификация и удаление пакетов приложений [1].

Система APT поддерживает формат хранилища программных пакетов — репозиторий пакетов.

Репозиторий представляет собой иерархическую (древовидную) структуру директорий. Такая структура аналогична структуре, которая используется в файловых системах ОС.

Хранение пакетов приложений в репозиториях имеет ряд преимуществ [1]:

– возможность размещения локально (например, на USB-носителе) на компьютере под управлением ОС СН Astra Linux SE или в сети.

– централизованное управление доступом и конфигурированием одновременно несколькими репозиториями;

– организация проверки подлинности устанавливаемых пакетов с использованием организации их цифровой подписи [2,3];

– организация доступа к содержимому репозиториев на основе механизма аутентификации с открытым ключом (public key).

Пакеты приложений обычно содержат все файлы необходимые для реализации определенного набора функций.

ОС СН Astra Linux SE поддерживает два типа пакетов:

1. Двоичные (Binary) пакеты, которые содержат выполняемые и конфигурационные файлы пакета, страницы справочной системы man, информацию об авторских правах и другую документацию. Эти пакеты распространяются в архивах специального формата и имеют расширение .deb.;

2. Исходные (Source) пакеты, которые состоят из трех компонент:

– файла с расширением .dsc для описания исходного пакета;

– сжатого архива с расширением .orig.tar.gz, содержит оригинальный исходный текст программы;

– сжатого файла с расширением .diff.gz, содержит специфические для ОС СН изменения к исходным текстам.

Команда dpkg (Debian PacKaGes) входит в состав системы управления пакетами APT и является менеджером пакетов начального уровня.

Функциями команды dpkg являются установка и удаление пакетов, а также отображение их статуса.

Основным набором команд, используемым для работы с репозиториями, является набор команд apt (advanced packaging tool).

Набор команд apt совмещает в себе функционал команды dpkg по работе с пакетами приложений и дополнительно содержит функции управления репозиториями.

Команда apt одновременно может работать с несколькими репозиториями.

Для поддержки информации об используемых репозиториях используется конфигурационный файл /etc/apt/sources.list.

Для настройки функционирования команд apt служат конфигурационные файлы:

etc/apt/apt.conf — основной файл конфигурации системы APT;

/etc/apt-move.conf — файл конфигурации путей к локально установленным на жестком диске репозиториям;

/etc/apt/preferences — файл предпочтений. В файле определено, какая версия пакета будет установлена в случае наличия в репозитории сразу нескольких его версий.

Полученные из репозиториев пакеты кэшируются в директории /var/cache/apt/archives.

В ОС СН Astra Linux SE (вер. 1.6) используются репозитории установочного диска (основной) и диска со средствами разработки.

В новой версии ОС СН Astra Linux SE (обновления 1.7) используются следующие репозитории: основной, базовый, расширенный.

В ОС СН Astra Linux SE (обновления 1.7) не допускается одновременное использование расширенного и основного/базового репозитория из разных версий оперативных обновлений.

Основной репозиторий.

Работа с репозиторием установочного диска в ОС СН Astra Linux SE (обновление 1.7) содержит ряд отличий от работы в Astra Linux (версия 1.6):

– диск со средствами разработки, (как в версии 1.6,) не используется, а вместо него необходимо использовать базовый репозиторий;

– подключение расширенного репозитория может повлиять на выбор устанавливаемых пакетов.

Базовый репозиторий.

Работа с базовым репозиторием Astra Linux SE (очередное обновление 1.7) в целом не отличается от работы в ОС СН Astra Linux SE (обновление 1.6) с подключенным репозиторием со средствами разработки, но необходимо обратить внимание на следующие особенности:

– базовый репозиторий содержит все пакеты основного репозитория, поэтому при использовании базового репозитория использование основного репозитория можно исключить;

– дополнительно базовый репозиторий содержит пакеты, относящиеся к средствам разработки;

– подключение расширенного репозитория может влиять на выбор устанавливаемых пакетов.

Расширенный репозиторий.

Пакеты, содержащиеся в расширенном репозитории, не дорабатываются для применения в ОС СН Astra Linux SE и не проходят сертификационные испытания, но технически могут обновлять или заменять пакеты, находящиеся в базовом репозитории.

Работа ПО, установленного из расширенного репозитория, как и любого другого ПО, контролируется общими правилами мандатного разграничения доступа (МРД) и мандатного контроля целостности (МКЦ), действующими в ОС СН [4]. При этом ОС СН может работать в любом режиме защиты, однако взаимодействие комплексов средств защиты с ПО может быть ограничено.

Расширенный репозиторий содержит пакеты ПО, не включенные в состав основного и базового репозиториев. ПО может быть несовместимо с пакетами из базового и расширенного репозиториев. Основное назначение расширенного репозитория — расширение инструментария основного и базового репозиториев. При этом пакеты, входящие в основной состав расширенного репозитория, не могут изменять (обновлять, удалять) пакеты, из состава основного репозитория, но могут изменять пакеты из состава базового репозитория.

Использование репозиториев в Astra Linux SE (очередное обновление 1.7) позволяет устанавливать и эксплуатировать ПО, разработанное для других Linux-систем, разрабатывать собственное ПО в среде разработки и переносить ОС СН Astra Linux SE на различные аппаратные платформы.

СПИСОК ЛИТЕРАТУРЫ

1. Деньжонков К. А. Основы построения и администрирования защищенной операционной системы специального назначения Astra Linux Special Edition : учебное пособие / К. А Деньжонков, А. В.Кий , В. В. Пащенко [и др.]. СПб. : ВАС, 2019. С. 116-127.
2. Ильина О. Б., Купчиненко О. П., Скоропад А. В. К вопросу о дополнительных средствах защиты информации в операционной системе специального назначения Astra Linux SE // Информационная безопасность регионов России: материалы XI Санкт-Петербургской международной конференции, СПб, 23-25 октября 2019 г. СПб : СПОИСУ, 2019. Т. 2. С. 224-226.
3. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О дополнительных задачах администрирования средств защиты информации в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2019. Т. 2. С. 318-323.
4. Ильина О. Б., Купчиненко О. П., Скоропад А. В. К вопросу об изменениях в системе защиты информации в операционных системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. СПб: СпбГУТ, 2021. С. 251-254.

УДК 621.39

МЕТОДИКА УПРАВЛЕНИЯ МАРШРУТИЗАЦИЕЙ В СЕТИ ПЕРЕДАЧИ ДАННЫХ ГРУППЫ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Кичко Яна Викторовна, Сапунова Лидия Петровна
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: kichkoyanka@mail.ru

Аннотация. Развитие групп беспилотных летательных аппаратов (БПЛА) и организация их работы являются основными научно-техническими направлениями, способствующими повышению эффективности систем, используемых в различных секторах национальной экономики. Процесс функционирования группы БПЛА осуществляется с помощью сети передачи данных (СПД), которая обеспечивает взаимодействие между объектами группы и внешними субъектами. В настоящее время в связи с особенностями свойств БПЛА, условиями их применения и влиянием радиопомех от других систем, актуальными являются задачи анализа и оптимизации помехозащищенных СПД для обеспечения гарантированного обмена сообщениями между объектами группы БПЛА. В рамках предложенной методики предусмотрено рассчитывать вероятность своевременной доставки сообщений в СПД при использовании различных типов модуляции и кодирования. Результаты этих расчетов могут быть использованы для обоснования технических решений по разработке и применению алгоритмов для формирования и обработки данных, а также для пакетной маршрутизации в СПД БПЛА с гарантированным соблюдением требований к своевременной доставке сообщений.

Ключевые слова: группа беспилотных летательных аппаратов, сеть передачи данных, маршрутизация пакетов, радиоподавление, оптимизированная помеха.

ROUTING MANAGEMENT METHODOLOGY IN DATA TRANSMISSION NETWORK FOR UNMANNED AERIAL VEHICLE GROUPS

Kichko Yana, Sapunova Lidiya
Military Academy of Communications Marshal of the Soviet Union S. M. Budyonny
Tikhoretsky Ave., 3, St. Petersburg, 194064, Russia
e-mail: kichkoyanka@mail.ru

Abstract. The development of groups of unmanned aerial vehicles (UAVs) and the organization of their work are the main scientific and technical areas that contribute to improving the efficiency of systems used in various sectors of the national economy. The process of functioning of a group of UAVs is carried out using a data transmission network (SDN), which provides interaction between the objects of the group and external entities. Currently, due to the peculiarities of the properties of UAVs, the conditions of their use and the influence of radio interference from other systems, the tasks of analyzing and optimizing noise-proof SPDs to ensure guaranteed messaging between objects of the UAV group are relevant. Within the framework of the proposed methodology, it is provided to calculate the probability of timely delivery of messages to the SPD using various types of modulation and coding. The results of these calculations can be used to substantiate technical solutions for the development and application of algorithms for the formation and processing of data, as well as for packet routing in the UAV SPD with guaranteed compliance with the requirements for timely delivery of messages.

Keywords: group of unmanned aerial vehicles, data network, packet routing, jamming, optimized interference.

В современном мире беспилотные летательные аппараты (БПЛА) становятся все более популярными и востребованными. Они нашли широкое применение в различных областях, таких как геодезия, аэрофотосъемка, доставка грузов, мониторинг и т.д. [1-3]. Однако, чтобы эффективно функционировать и выполнять поставленные задачи, группе БПЛА требуется надежная и эффективная сети передачи данных (СПД), которая необходима для обеспечения обмена данными и взаимодействия всех объектов сети [2, 3].

Алгоритмы маршрутизации являются важной компонентой, обеспечивающей оптимальное распределение и передачу данных между БПЛА в сети. Эти алгоритмы определяют наилучшие пути передачи информации, учитывая различные факторы, такие как пропускная способность каналов, расстояние, время задержки и прочие параметры.

Одной из главных проблем, стоящих перед сетями БПЛА, является ограниченная пропускная способность каналов связи. Каждый БПЛА генерирует большой объем данных, включая сведения о состоянии, координатах, изображениях и видеопотоках. Неэффективная маршрутизация может привести к перегрузке каналов и задержке передачи данных, что в свою очередь негативно сказывается на работе БПЛА и их способности выполнять поставленные задачи. Быстрое устаревание находящейся в БПЛА информации обуславливает высокие требования к допустимому времени доставки сообщений получателям, которое в зависимости от типов данных и взаимодействующих объектов может составлять секунды и менее [2, 3]. При этом эффективность функционирования группы БПЛА и ее физическое состояние напрямую зависят от степени обеспечения системой связи требуемых показателей обмена сообщениями между объектами.

Еще одна важная проблема связана с надежностью и безопасностью передачи данных. Беспилотные летательные аппараты часто используются в критически важных областях, таких как поисково-спасательные операции или медицинская помощь, где недостаточная надежность связи может иметь серьезные последствия. Правильно спланированные и эффективные алгоритмы маршрутизации позволяют обеспечить надежную и безопасную передачу данных между БПЛА, минимизируя возможные сбои или задержки.

Наконец, вместе с развитием БПЛА появляется необходимость в интеграции их с другими системами, такими как наземные станции управления, системы навигации и др. Алгоритмы маршрутизации становятся ключевым компонентом в создании сетей, которые обеспечивают эффективную и безопасную работу всей системы.

Исследование СПД группы БПЛА получает большое внимание из-за важности рассматриваемых вопросов. Анализ и оптимизация СПД являются приоритетными задачами [1-3], также изучается влияние различных факторов на функционирование системы [2].

Также актуальным является разработка устойчивых принципов построения СПД, включая критерии связности сети, вероятность обмена данными и другие показатели [2, 3].

Таким образом, актуальность разработки алгоритмов маршрутизации для СПД группы БПЛА невозможно недооценить. Эти алгоритмы играют решающую роль в обеспечении эффективности, надежности и безопасности передачи данных между БПЛА.

В данной работе предлагается методика управления маршрутизацией в СПД группы БЛА при наличии оптимизированных помех, то есть помех, которые максимально влияют на систему при ограничениях на мощность источника помехи. Такой подход позволяет провести проектирование СПД с учетом заданных ограничений и оценить достижимые показатели эффективности, а также определить параметры СПД, которые удовлетворят требованиям к скорости передачи данных.

Цель работы — представить методику управления маршрутизацией в СПД группы БПЛА в классе возможных помех при ограничении на мощность источника помехи (ИП) и обоснования параметров СПД, обеспечивающих необходимую скорость передачи данных.

Постановка задачи. При решении исследуемой задача полагаем, что ИП оптимальным образом распределяет энергетический ресурс помехи на сетевом уровне СПД с учетом ее оптимизированного воздействия на физическом и канальном уровнях. В качестве критерия оптимальности СПД будем использовать показатель, характеризующий вероятность своевременной доставки сообщений в сети. Поскольку данный показатель, аналогично [3], пересчитывается к соответствующей вероятности своевременной доставки пакетов данных, задача сводится к решению оптимизационной задачи, которую удобно рассматривать в рамках игры на множествах стратегий первого игрока — системы (СПД) и второго игрока — контрсистемы (ИП) с функцией выигрыша (первого игрока) [3, 4]. Для заданной конструкции сети гарантированная в классе помех с ограниченной мощностью вероятность своевременной доставки, соответствует нижней цене игры, обеспечиваемой стратегией первого игрока. Участвующие в задачекомпоненты формализуются при описании модели взаимодействия СПД и ИП.

Определенный показатель помехозащищенности характеризует максимальную мощность ИП, при которой СПД гарантированно обеспечивает требуемую вероятность своевременной доставки сообщений объектам группы БПЛА.

Для решения задачи приходится декомпозировать модель взаимодействия СПД группы БПЛА с ИП на 3 уровня — физический, канальный и сетевой [5].

Разработанная методика управления маршрутизацией основана на алгоритме нахождения варианта помехи, которая при заданной мощности минимизирует вероятность своевременной доставки сообщений в СПД. Она включает в себя модули расчета показателей, характеризующих работу объектов СПД на различных уровнях ее функциональной архитектуры и содержит процедуры оптимизации распределения помехи на физическом и сетевом уровнях, а также отдельных параметров СПД. Так, для канала передачи данных решаются задачи оптимизации «тонкой» структуры помехи, т.е. распределения мощности в классе помех, и базы псевдослучайного сигнала в радиолиниях, а на сетевом уровне — распределения мощности ИП по объектам СПД и системы маршрутных таблиц.

Разработанная методика позволяет оценить, насколько быстро сообщения доставляются в СПД группы БПЛА. Результаты исследования своевременности передачи данных позволяют выявить проблемы, которые могут возникнуть в работе СПД, и принять соответствующие технические решения. Эти результаты будут исследоваться дальше для оптимизации алгоритмов оценивания состояния радиолиний, управления параметрами сигналов и алгоритмов кодирования/декодирования, а также разработки эффективных процедур взаимодействия между отправителями и получателями данных в процессе обмена информацией.

СПИСОК ЛИТЕРАТУРЫ

1. Bujari A. Flying ad-hoc network application scenarios and mobility models / A. Bujari, C. T. Calafate, J. C. Cano, P. Manzoni [et al] // International Journal of Distributed Sensor Networks. 2017. Vol. 13. № 10. P. 1–17. DOI: 10.1177/1550147717738192.
2. Wen S., Huang C. Delay-constrained routing based on stochastic model for flying ad hoc networks // Mobile Inf. Syst. 2018. DOI: 10.1155/2018/6056419.
3. Чуднов А. М., Губская О. А., Кичко Я. В. Методика анализа вероятностно-временных характеристик обмена сообщениями в комплексе беспилотных летательных аппаратов // Известия ТулГу. Технические науки. 2021. № 11. С. 117–124.
4. Чуднов А. М. Математические основы моделирования, анализа и синтеза систем. СПб : ВАС. 2021. 193 с.
5. Чуднов А. М., Положинцев Б. И., Кичко Я. В. Анализ помехозащищенности обмена данными группы беспилотных летательных аппаратов в условиях оптимизированных помех // Радиотехника. 2022. Т. 86. № 12. С. 33-47.

УДК 004.03

ПОКАЗАТЕЛИ КАЧЕСТВА И БЕЗОПАСНОСТИ КОНТЕНТА ЭЛЕКТРОННЫХ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ В ИНТЕРЕСАХ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ИНЖЕНЕРНОГО ПРОФИЛЯ

Крюкова Елена Сергеевна, Паращук Игорь Борисович
Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: e.kkrukovaa69@yandex.ru, shchuk@rambler.ru

Аннотация. В докладе рассмотрены некоторые показатели качества и безопасности контента электронных образовательных ресурсов, используемых в процессе подготовки специалистов инженерного профиля. Определены базовые понятия электронных образовательных ресурсов и достоинства их применения в учебном процессе. Перечислены некоторые требования к контенту электронных образовательных ресурсов. Описаны его свойства, предложены показатели качества для их количественной оценки.

Ключевые слова: контент, электронные образовательные ресурсы, показатель качества, специалисты инженерного профиля, безопасность, информационные и телекоммуникационные системы, требования к контенту.

CONTENT QUALITY AND SAFETY INDICFTORS ELECTRONIC EDUCATIONAL RESOURCES FOR THE INTEREST OF TRAINING ENGINEERING SPECIALISTS

Kryukova Elena, Parashchuk Igor
Military Academy of Communications Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails: e.kkrukovaa69@yandex.ru, shchuk@rambler.ru

Abstract. The report discusses some indicators of the quality and safety of the content of electronic educational resources used in the process of training engineering specialists. The basic concepts of electronic educational resources and the advantages of their use in educational process. Some requirements for the content of electronic educational resources are listed. Its properties are described, quality indicators for their quantitative assessment are proposed.

Keywords: content, electronic educational resources, quality indicator, engineering specialists, security, information and telecommunication systems, content requirements.

Использование информационных и телекоммуникационных технологий (ИТКТ) в процессе подготовки специалистов инженерного профиля (СИП) в настоящее время достаточно актуально и постоянно находит все более широкую область применения систем такого класса. Средством обучения в ИТКТ является электронный образовательный ресурс (ЭОР), который представляет собой электронный образовательный контент, состоящий из нормативных, информационных, программных средств, технических и методических материалов, аудио и видеоматериалов, полнотекстовых электронных изданий, иллюстративных материалов, каталогов электронных библиотек. Также термин «электронные образовательные ресурсы» объединяет весь спектр средств обучения, которые разработаны и воспроизводятся на базе компьютерных технологий [1].

Одним из достоинств использования ЭОР в образовательной деятельности является интенсификация процесса освоения обучающимися содержательной части определенной предметной области, в нашем случае технических дисциплин, за счет приобретения ими умения самостоятельно осуществлять информационную деятельность (возможность поиска информации по определенным признакам, ее обработки и представления в различном виде, управления экранным отображением моделей изучаемых объектов или процессов и т.д.). Неоспоримое преимущество применения ЭОР в образовательном процессе — это наличие возможности осуществлять дистанционное обучение.

Базовым (ключевым) понятием ЭОР является его контент, то есть содержательная часть, ориентированная на удовлетворение потребностей обучающихся в процессе освоения ими учебного материала.

Контент — это информация и иное содержимое, доводимое до пользователя через его органы чувств с помощью пользовательского приложения [2].

Другим основополагающим понятием, при рассмотрении ЭОР, является его качество — совокупность педагогико-эргономических свойств, направленных на удовлетворение потребностей обучающихся и на повышение эффективности процесса обучения СИП [3]. Для определения качества контента ЭОР к нему могут быть предъявлены следующие требования: содержательно-методические, технико-технологические и дизайн-эргономические. При этом под одним из содержательно-методических требований следует понимать необходимость создания условий для обеспечения вариативности обучения, в том числе дистанционного. В части технико-технологических требований можно отметить необходимость обеспечения возможности доступа к контенту ЭОР и работы с ним с различных устройств. Формулируя дизайн-эргономические требования следует обратить внимание на обеспечение возможности реализации технологии мультимедиа в процессе интерактивного взаимодействия обучающихся с ЭОР. Также предъявляются требования к уровню подготовки педагогов, которые должны владеть современными ИТКТ, применяемыми в процессе подготовки СИП и другие требования [4].

К наиболее значимым свойствам контента ЭОР можно отнести полезность (информация должна нести пользу для обучающегося), соответствие запросу (информация должна удовлетворять запрос пользователя), правдивость (информация не должна быть ложной или вводить пользователя в сомнения), разнообразие (информация должна быть представлена в разных форматах и освещать различные темы), вредоносность (уровень вреда, возможного негативного влияния на мировоззрение, психологию и здоровье обучаемого), актуальность (информация должна соответствовать времени) и грамотность (информация должна быть без ошибок) [5].

Для возможности аналитического описания свойств контента ЭОР будем использовать их количественную меру — показатели качества (ПК) [6].

В качестве ПК полезности контента ЭОР в интересах подготовки СИП может рассматриваться коэффициент полезности, представляющий собой соотношение количества информации, которая приносит пользу обучающимся и времени, которое было затрачено на ее нахождение. Полезность контента ЭОР ориентирована прежде всего на удовлетворение потребностей будущих СИП.

Соответствие контента запросам пользователей можно оценить с помощью такого ПК как коэффициент релевантности. Под релевантностью контента понимается степень соответствия найденного контента запросам пользователя. Количественно релевантность выражается через коэффициент равный проценту соответствия содержания контента ЭОР его запросу.

Разнообразие контента может быть оценено коэффициентом информативности. Это отношение количества новой информации к общему количеству информации, представленной в разных форматах и отражающей различные аспекты изучаемого материала.

Вредоносность контента ЭОР — это процент соответствия его содержания к наличию нежелательной информации, которая может оказать негативное влияние на обучающихся. Для избегания этого учебным заведениям необходимо использовать систему фильтрации («черный список» ресурсов, особенно внешних, с нежелательным контентом).

В качестве показателя актуальности контента может быть выбран коэффициент актуальности равный отношению количества контента ЭОР, размещенного в ИТКТ, допустим за последние 5 лет к общему количеству контента.

Отдельно необходимо отметить такое свойство ИТКТ и контента ЭОР как их безопасность.

Безопасность предоставления услуг ИТКТ — это свойство, характеризующее их способность противостоять несанкционированному доступу к контенту ЭОР, а также получению, уничтожению и (или) его изменению.

Безопасность контента ЭОР — это свойство или совокупность свойств контента, обуславливающих защищенность содержания потоков информации, передаваемых из образовательной организации в Интернет и получаемых из глобальной сети в локальную сеть образовательной организации [7-9].

Показателями качества безопасности предоставления услуг ИТКТ и контента ЭОР могут быть время вскрытия структуры и паролей легальных (авторизированных) пользователей, коэффициент конфиденциальности, который характеризует конфиденциальность предоставления контента ЭОР ИТКТ, время восстановления сетевых паролей после компрометации [10].

Таким образом, проведен анализ понятий ЭОР, его контент, качество и безопасность, отмечены достоинства применения ЭОР в образовательном процессе. Предпринята попытка сформулировать некоторые требования к контенту. Описаны его свойства и возможные ПК с помощью которых он может быть оценен. Дальнейшим направлением исследования нам видится разработка системы ПК контента ЭОР включающей как можно большее количество показателей для всестороннего описания его свойств, создание моделей и методов адаптивного мониторинга контента ЭОР с целью подготовки СИП в высших учебных заведениях.

СПИСОК ЛИТЕРАТУРЫ

1. Юдин А. А., Чирушкин К. А., Ренсков А. А. Методические рекомендации по разработке электронных учебников и учебных пособий. СПб.: ВАС, 2017. 163 с.
2. ГОСТ Р 52872-2019. Национальный Стандарт Российской Федерации. Интернет-ресурсы и другая информация, представленная в электронно-цифровой форме. Приложения для стационарных и мобильных устройств, иные пользовательские интерфейсы. 2019.
3. Петухов Г. Б. Основы теории эффективности целенаправленных процессов. Ч. 1. М.: МО СССР, 1989. 660 с.
4. Климович Н. Г. Контент: топовые техники SEO-продвижения. М.: Инфра-Инженерия. 2021. 330 с.
5. Евстратова Е. Что такое контент — объяснение английского термина русскими словами // Что такое контент. 2020. [Электронный ресурс]. URL: https://elenaevstratova.ru/chto-takoe-kontent/ (дата обращения: 27.05.2023).
6. Сейдж Э., Мэлс Дж. Теория оценивания и ее применение в связи и управлении. М.: Связь, 1976. 496 с.
7. Ганжур А. П., Отакулов А. С., Дьяченко Н. В. Политика безопасности контента // Молодой исследователь Дона. № 6 (33), 2021. С. 41-44.
8. Котенко И. В., Саенко И. Б., Браницкий А. А., Паращук И. Б., Гайфулина Д. А. Интеллектуальная система аналитической обработки цифрового сетевого контента для защиты от нежелательной информации // Информатика и автоматизация (Труды СПИИРАН). Вып. 20(4), 2021. С. 755-792.
9. Десницкий В. А., Котенко И. В., Паращук И. Б. Методика оценки эффективности систем обработки сетевого контента для обнаружения вредоносной информации с учетом устранения неопределенности смыслового наполнения информационных объектов // XXII Международная конференция по мягким вычислениям и измерениям (SCM-2019) : сборник докладов. Санкт-Петербург, 23-25 мая 2019 г. СПб.: СПбГЭТУ «ЛЭТИ», 2019. С. 62-65.
10. Паращук И. Б., Крюкова Е. С., Михайличенко Н. В. Особенности и принципы оптимального адаптивного мониторинга центров обработки данных и электронных библиотек // Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конференции. Севастополь, 22-26 сентября 2020 г. Севастопольский государственный университет // науч. ред. Б. В. Соколов. Севастополь: СевГУ, Т. 2, 2020. С. 47-48.

УДК 621.391 (075.8)

О ПРАВАХ ПОЛЬЗОВАТЕЛЯ В ОПЕРАЦИОННОЙ СИСТЕМЕ

Купчиненко Ольга Павловна[1], Ильина Ольга Борисовна[1], Скоропад Александр Витальевич[2]
[1]Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
[2]Санкт-Петербургский филиал — «ЛОНИИР» (ФГБУ НИИР),
Большой Смоленский пр., 4, Санкт-Петербург, 192029, Россия
e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Аннотация. В операционной системе специального назначения Astra Linux SE применение дополнительных средств защиты информации позволяет построить более гибкую и надежную систему защиты от несанкционированного доступа. Для дополнительного ограничения прав пользователей используется режим Киоск. Рассмотрены особенности обновленной версии режима Киоск-2.

Ключевые слова: операционная система специального назначения; защита информации; средства защиты информации; пользователь; профиль пользователя; права доступа.

ABOUT USER RIGHTS IN THE OPERATING SYSTEM

Kupchinenko Olga[1], Ilina Olga[1], SkoropadAleksandr[2]
[1]The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
[2]The M.I. Krivosheev Radio Research & Development Institute. LENINGRAD BRANCH — «LONIIR»
4 Bolshoy Smolensky Av, St. Petersburg, 192029, Russia
e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Abstract. In the operating systems of a special purpose Astra Linux SE, the use of additional information security tools allows you to build a more flexible and reliable system of protection against unauthorized access. Kiosk mode is used for additional restriction of user rights. The features of the updated version of the Kiosk-2 mode are considered.

Keyword: operating system of a special purpose; information security; information security tools; user; user profile; access rights.

Защита информации в современных операционных системах должна быть комплексной и должна предусматривать обеспечение физической целостности информации, предупреждение несанкционированной ее модификации и предотвращение несанкционированного получения.

Функциональные возможности современной операционной системы специального назначения (ОС СН) Astra Linux SE расширены комплексом средств защиты, реализующим дополнительные функции администрирования системы [1, 2].

Режим Киоск служит для ограничения прав пользователей в ОС СН.

Режим Киоск является реализованным в системе защиты информации (СЗИ) PARSEC вариантом маски umask. Отличительной особенностью режима Киоск является то, что при использовании команды umask маска на разрешения накладывается только при создании новых объектов файловой системы, а при применении режима Киоск маска на разрешения к объектам файловой системы накладывается при любой попытке пользователя получить доступ. Маска режима Киоск применяется только к файлам обычного типа. К директориям, сокетам и файлам устройств маска режима Киоск не применяется [3].

Режим Киоск-2 — это новый инструмент PARSEC, заменяющий режим Киоска. Работу режима Киоск-2 обеспечивает пакет parsec-kiosk2. Пакет parsec-kiosk2 содержит инструменты для ограничения возможностей, которые предоставляются непривилегированным пользователям, это обновлённая версия пакета parsec-kiosk. Пакет parsec-kiosk2 входит в состав обновления ОС СН Astra Linux SE Смоленск версии1.6 № 20190912SE16 и последующие обновления.

Новый пакет устанавливается по умолчанию при установке обновления. Установка пакета возможна так же на любой операционной системе Astra Linux (в том числе на Astra Linux Common Edition).

Дополнительно при установке пакета parsec-kiosk2 устанавливается обновлённый графический инструмент для управления профилями fly-admin-kiosk. После установки он доступен через систему графического меню.

Системный киоск (fly-admin-kiosk) — это графическое приложение для управления ограничениями пользователя.

Инструмент позволяет включать и отключать режим киоска двумя способами:

– через графическое меню;
– кнопкой с изображением ключей.

Кроме того, средство fly-admin-kiosk позволяет изменять содержимое файлов профилей.

Создавать и изменять профили пользователей можно разными способами:

– включением в профиль пользователя стандартных профилей;

– генерацией набора файлов из трассировки приложения, выполняемого от имени пользователя (кнопка Добавить файлы из);

– копированием существующего (типового) профиля пользователя.

Пакет fly-admin-kiosk не требует предварительной настройки и позволяет:

– включать/выключать режим Киоск-2, протоколирование процессов в режимах настройка трассировки процесса или глобальной загрузочной записи, профили пользователей;

– создавать и редактировать профили с помощью включения в профиль пользователя стандартных профилей;

– копировать, удалять профили пользователей;

– отменять изменения в профилях.

Файлы с профилями parsec-kiosk2 располагаются в каталоге /etc/parsec/kiosk2-profiles. При установке пакета в этот каталог устанавливается набор типовых профилей.

Киоск-2 ограничивает только тех пользователей, для которых создан профиль в /etc/parsec/kiosk2.

Синтаксис профилей Киоск-2 отличается от синтаксиса профилей Киоск. При этом, parsec-kiosk2 распознает синтаксис профилей parsec-kiosk. Профиль, содержащий строки, написанные каждым синтаксисом, будет корректно работать в режиме Киоск-2.

Синтаксис профилей Киоска-2.

1. Базовый.

Команда:

+file <r/w/c> <u/o>: <filename>

разрешает чтение/изменение/создание файловых объектов владельцу/не владельцу [4]. В имени файла могут использоваться метасимволы, например:

+file ? u: ** (разрешить создание, запись, чтение владельцам файлов).

Вариант команды с чтением ссылки:

+link <r/w/c> <u/o>: <filename>

Имя файла должно соответствовать существующей символьной ссылке. Целевой файл для ссылки (который не обязан существовать в момент загрузки профиля) добавляется в список доступных файлов.

2. Совместимый с parsec-kiosk.

«/file/name» rwx

/file/name rwx

«/file/name» r-x

/file/name -w-

В этом случае:

– имя файла считается литералом (спецсимволы не интерпретируются);

– любое из прав r/x преобразуется в r, w преобразуется в wc;

– правила применяется одинаково и для доступа владельцев и для доступа остальных;

– строка обязательно должна начинаться с символа кавычки или символа «слэш»;

– если файл представляет символьную ссылку, в вывод профиля попадает целевой файл ссылки.

Для включения файла в профиль (совместимый со старой версией Киоск) необходимо выполнить:

other-profile-name

Имя включаемого файла обязано начинаться с латинской буквы, символы «слэш» в имени не допускаются.

Режим Киоск-2 имеет независимые глобальные переключатели для применения ограничений к пользователям и для протоколирования запрещённых действий ядром ОС СН (режим протоколирования также применяется для создания новых профилей).

Режим Киоск-2 включает протоколирование с сохранением исходного состояния системы до перезагрузки ОС СН и после перезагрузки. Режим Киоск протоколирование не включает.

Режим Киоск-2 является средством ограничения прав пользователей в ОС СН Astra Linux SE, версии 1.6 и позволяет создать безопасный профиль пользователя с соблюдением всех требований по защите информации.

СПИСОК ЛИТЕРАТУРЫ

1. Ильина О. Б., Купчиненко О. П., Скоропад А. В. К вопросу о контроле целостности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. СПб: СпбГУТ, 2022, Т. 2, С. 243-248.
2. Ильина О. Б., Купчиненко О. П., Скоропад А. В. К вопросу о дополнительных средствах защиты информации в операционной системе специального назначения Astra Linux SE // Информационная безопасность регионов России : материалы XI Санкт-Петербургской международной конференции, СПб, 23-25 октября 2019 г. СПб.: СПОИСУ, 2019. Т. 2. С. 224-226.
3. .Ильина О. Б., Купчиненко О. П., Скоропад А. В. О дополнительных задачах администрирования средств защиты информации в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2019. Т. 2. С. 318-323.
4. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. СПб.: СПбГУТ, 2018. Т. 2. С 356-360.

УДК 004.056

РЕАЛИЗАЦИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ СЕТИ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ ПРОГНОЗИРОВАНИЯ ДЕЙСТВИЙ НАРУШИТЕЛЯ

Липатников Валерий Алексеевич[1], Шевченко Александр Александрович[2], Мелехов Кирилл Витальевич[1]

[1] Военная академия связи имени Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, г. Санкт-Петербург, 194064, Россия

[2] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия

e–mails: lipatnikovanl@mail.ru, alex_pavel1991@mail.ru, kirill_melehov@bk.ru

Аннотация. В докладе представлено предложение по реализации проактивного управления информационной безопасностью сети передачи данных. В основе предлагаемого способа лежит прогнозирование стратегии вторжения нарушителя за счет применения интеллектуальных технологий как на этапе формирования прогноза, так и на этапе анализа цифрового потока и выявления признаков воздействия на сеть.

Ключевые слова: информационная безопасность, сеть передачи данных, интеллектуальные технологии.

IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT OF THE DATA NETWORK BASED ON THE PREDICTION OF THE ACTIONS OF AN INTRUDER

Lipatnikov Valery[1], Shevchenko Alexander[2], Melekhov Kirill[1]

[1]The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

[2] The Bonch-Bruevich Saint-Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia

e–mails: lipatnikovanl@mail.ru, alex_pavel1991@mail.ru, kirill_melehov@bk.ru

Abstract. The report presents a proposal for the implementation of proactive information security management of the data transmission network. The proposed method is based on predicting the intruder's intrusion strategy through the use of intelligent technologies both at the stage of forecast formation and at the stage of analyzing the digital stream and identifying signs of impact on the network.

Keywords: information security, data network, intelligent technology.

С эволюцией телекоммуникационных сетей и информационных технологий изменялись условия взаимодействия пользователя и вычислительной техники. Информация, циркулирующая в информационные системы, приобретала все большие объемы и влияние на разные сферы деятельности человека. При этом развивалась в соответствии с прогрессом информационных технологий и учетом возникающих угроз и новых видов воздействий на сети передачи данных (СПД).

В [1] рассматривается подход к разработке и использованию систем информационной безопасности (ИБ), основанный на выделении интеллектуальной надстройки над традиционными способами защиты и построении единой унифицированной среды для создания и поддержки функционирования систем защиты. В [2] рассматриваются вопросы модификации процесса генерации модели атак и методики его анализа для более адекватного мониторинга и выбора защитных мер. В [3] описан подход к анализу информационных рисков с применением нечеткого когнитивного подхода в сочетании с использованием искусственных нейронных сетей. Вопросы, рассмотренные в указанных работах, не затрагивают обнаружение вторжений нарушителя и анализ его действий.

В связи с этим целью исследования является повышение вероятности защищенности СПД в течение заданного времени путем разработки способа проактивного управления безопасностью с прогнозом стратегии вторжения нарушителя за счет применения интеллектуальных технологий.

Таким образом, в рамках поставленной задачи, целесообразно разработать новую модель информационной сети в условиях динамики угроз вторжения с использованием интеллектуальных технологий аналитики, прогнозирования и реагирования на инциденты. Предполагается, что каждый сегмент сети выходит в WAN через межсетевой экран, обеспечивающий защиту периметра от атак. Для обеспечения конфиденциальности и целостности данных передача производится посредством построения VPN-туннелей, которые конфигурируются на VPN-серверах [4]. Чтобы обеспечить работу сети (маршрутизацию ip-пакетов), в инфраструктуру добавлены маршрутизаторы. А чтобы увеличить количество подключенных устройств и разбиение сети на сегменты подсети используются коммутаторы.

Для обеспечения возможности интеллектуальной автоматизации, удобства управления, мониторинга и проактивной защиты от вторжения нарушителя необходимо внедрить сервер безопасности, который будет находиться в головном офисе и обеспечивать вышеперечисленные функции во всей сети [5].

Алгоритм подразумевает описание полного цикла управления безопасностью СПД. Ниже представлено подробное описание работы алгоритма.

1. Алгоритм начинается со входа в цикл управления уже функционирующей сети передачи данных.
2. Далее, согласно топологии и настроек информационно-телекоммуникационной сети, происходит сбор и анализ данных с занесением в базу актуального состояния системы.
3. После происходит анализ цифрового потока, собранного системой мониторинга и сбора информации.
4. Далее следует блок распознавания вторжений посредством использования классификаторов.
5. После этого происходит опрос системы на наличие аномалий и, если они есть, определяется событие ИБ.
6. Далее события относятся к инцидентам ИБ, что отражается в алгоритме в данном блоке.
7. Следующим шагом система определяет критичность влияния инцидента ИБ на информационную защищенность СПД и при некритичном влиянии происходит корректировка конфигураций оборудования и ПО и сохранение данных. После чего алгоритм переходит к блоку №2.
8. Затем выполняется классификация инцидента и добавление данных о нем в базу безопасности [6].
9. После производится определение причины возникновения компьютерной атаки посредством анализа входных данных.
10. Следующим этапом работы алгоритма является выработка стратегии нейтрализации компьютерной атаки.
11. Условие дальнейшего продолжения работы алгоритма — разработана ли стратегия нейтрализации атаки СПД. Если данная атака уже встречалась системе и данные о ней имеются в базе угроз, система уточняет необходимо ли привлечение администратора к разрешению атаки.
12. Если необходимо решение администратора, то, согласно данному блоку, система ожидает от него действий. Администратор производит дополнительный поиск методов и мер, применяет имеющиеся знания и навыки для борьбы с компьютерной атакой. Иначе, в отсутствие мер противодействия, злоумышленник добьется желаемого результата и нарушит устойчиво безопасное функционирование СПД, нанесет вред или произведет кражу данных.
13. Если необходимость привлечения администратора отсутствует, то производится корректировка данных и устранение компьютерной атаки в автоматическом режиме.
14. Данный блок работает, если возникшая атака не встречалась системе и стратегия ее нейтрализации неизвестна, разработать ее не получается. В таком случае производится принятие мер по оповещению администратора ИБ и минимизации ущерба для СПД.
15. Следующим этапом является внесение изменений, принятых системой согласно стратегии нейтрализации атаки, в систему управления ИБ СПД.
16. Далее система проверяет произошла ли ликвидация атаки. Если системе или администратору не удалось ликвидировать компьютерную атаку на СПД, то алгоритм переходит к блоку №8. Если атаку удалось ликвидировать, то система управления ИБ формирует отчет для администратора, где отображает всю собранную информацию о произошедшем инциденте в удобной для восприятия форме. Данный отчет может сохраняться на носитель информации или отправляться посредством электронной почты.
17. После этого проводится диагностика системы и данные об инциденте ИБ добавляются в базу данных угроз. База данных системы обнаружения вторжений представляет собой реляционную систему взаимосвязанных таблиц, которая включает в себя все известные угрозы, включая в себя общедоступные БД, например, базу данных угроз «федеральной службы по техническому и экспортному контролю».
18. Данный блок означает конец цикла управления ИБ СПД. Цикл управления работает непрерывно и подразумевает собой постоянное обеспечение процесса защиты. Цикл и алгоритм заканчивают свое функционирование с выводом системы управления безопасностью СПД из эксплуатации.

Эффективность СУИБ СПД заключается в соотношении между достигнутым уровнем ИБ, полученным при управлении на основе СУИБ, и использованными ресурсами, обеспечившими его получение. Оценка эффективности СУИБ СПД должна осуществляться в рамках системного процесса получения и оценки объективных данных о текущем состоянии СУИБ, процессах и событиях, происходящих в ней, устанавливающего уровень их соответствия определенным организацией критериям. Разработанный алгоритм позволяет обеспечить требуемую эффективность.

СПИСОК ЛИТЕРАТУРЫ

1. Липатников В. А., Шевченко А. А., Яцкин А. Д. Метод управления безопасностью информационно-вычислительных сетей на основе выделенного сервера с контейнерной виртуализацией // Информационные системы и технологии. 2017. № 4(102). С. 116-126.
2. Коршунов Г. И., Липатников В. А., Шевченко А. А., Малышев Б. Ю. Метод адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя // Информационно-управляющие системы. 2018. № 4(95). С. 61-72.
3. Липатников В. А., Тихонов В. А., Шевченко А. А. Метод управления кибернетической безопасностью в системах критических инфраструктур, основывающийся на интеллектуальных сервисах защиты информации // Технологии построения когнитивных транспортных систем. Всероссийская научно-практическая конференция с международным участием, Санкт-Петербург, 28–29 мая 2019 г. : материалы конференции. СПб : Институт проблем транспорта им. Н. С. Соломенко РАН, 2019. С. 207-214.
4. Федорченко Е. В. Новикова Е. С., Гайфулина Д. А., Котенко И. В. Построение профиля атакующего на основе анализа сетевого трафика в критических инфраструктурах // Системы управления, связи и безопасности. 2021. № 6. С. 76-89.
5. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 1. С. 70-76.
6. Шевченко А. А. Предложения по построению упреждающей системы управления информационной безопасностью информационной системы // Инновационная деятельность в Вооруженных Силах Российской Федерации : Труды всеармейской научно-практической конференции, Санкт-Петербург, 14–15 октября 2020 г. СПб: ФГКВОУВО «Военная академия связи имени Маршала Советского Союза С. М. Буденного» МО РФ, 2020. С. 248-256.

УДК 621.396.67

АНАЛИЗ ПРИЧИН ИСКАЖЕНИЯ ДИАГРАММЫ НАПРАВЛЕННОСТИ БОРТОВЫХ ШИРОКОПОЛОСНЫХ АНТЕНН

Лянгузов Данила Андреевич
Военная академия связи имени Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: danilalgz@ya.ru

Аннотация. В докладе представлен анализ причин искажения характеристики направленности бортовой антенны в дальней зоне. Сформулированы рекомендации по снижению влияния вторичных токов, возникающих в ближней зоне бортового излучателя.

Ключевые слова: бортовые антенны; ближняя зона; диаграмма направленности; вторичный ток.

ANALYSIS OF THE CAUSES OF DISTORTION OF THE DIRECTIONAL PATTERNS BROADBAND ANTENNAS

Lyanguzov Danila
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: danilalgz@ya.ru

Abstract. The report presents an analysis of the reasons for the distortion of the onboard directivity antennas in the far field and formulated recommendations to reduce influence secondary currents of the near zone of the onboard emitter.

Keywords: on-board antennas, near-field, radiation pattern; secondary current.

В данном докладе проанализируем причины искажения диаграммы направленности (ДН) бортовых широкополосных антенн и сформулируем рекомендации по снижению влияния неравномерностей корпуса подвижного объекта (ПО) на форму ДН.

При работе бортовых антенн с нижней точкой питания на корпусе ПО возникают вторичные токи. От кромок и углов токопроводящего корпуса вторичные токи складываются с токами ближней зоны антенны. Это приводит к искажению ДН в определенном угловом секторе. В проведенном исследовании были проанализированы ДН конического несимметричного вибратора с нижней точкой питания, установленного на корпусе микроавтобуса в геометрическом центре ПО.

Расчет токов ближней зоны проведен методом конечных элементов, а ДН построена пересчетом токов из ближней в дальнюю зоны методом Стреттона-Чу [1, 2]. Если смещать антенну в сторону произвольной кромки корпуса ПО, плотность вторичных токов изменится, что приведет к перераспределению токов ближней зоны антенны, искажая ДН. Причем в диапазоне рабочих частот величина изменения плотности вторичных токов зависит от расстояния до неравномерности корпуса.

Для компенсации искажения токов ближней зоны целесообразно использовать такие излучатели, размер которых сопоставим с теоретически рассчитанным размером ближней зоны антенны. Например, ДН дискоконусной антенны с верхней емкостной нагрузкой в виде кольца в диапазоне частот искажается на 30 — 40 % меньше, чем у конусной антенны.

Однако, использование подобной конструкции в некоторых диапазонах частот (например, в ультракоротковолновом) может быть затруднительно вследствие громоздкости конструкции. Известны антенные системы [3], позволяющие формировать предыскаженную ДН. Исследование по анализу формы ДН подобных антенн можно представлено в работе [4]. В данном случае целесообразно использовать излучатели сложной формы, применяя емкостные вставки в местах наибольшей концентрации токов [5].

СПИСОК ЛИТЕРАТУРЫ

1. Jin J. The finite element method in electromagnetics. Wiley. 2014. 800 p.
2. Young W., Kwon Hyochoong Bang. The Finite Element Method using MATLAB. CRC Press LLC. 1997. 519 p.
3. Шанин А. М. Взаимное влияние элементов защищенных активных фазированных антенных решёток // Теория и техника радиосвязи. В., 2022. № 4. С. 73-79.
4. Шанин А. М. Модель передающего радиоцентра на основе принципа электродинамического подобия // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. СПб., 2023. № 5-6(179-180). С. 71-78.
5. Yijing H., Yue L. Dual-polarized microstrip antennas with capacitive via fence for wide beamwidth and high isolation // IEEE Transactions on Antennas and Propagation. 2020. Vol. 67. № 7. P. 5095-5103.

УДК 004.71

ИСПОЛЬЗОВАНИЕ МАРШРУТИЗАТОРОВ MIKROTIK ПРИ ПОСТРОЕНИИ ЗАЩИЩЕННЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Мандрик Дмитрий Владимирович, Сазонов Виктор Викторович
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: mandrick2013@yandex.ru, vmktor-sazonov@yandex.ru

Аннотация. Использование маршрутизаторов MikroTik для отработки построения защищённых сетей передачи данных, позволит сформировать у администраторов понимание ряда вопросов обеспечения безопасности.

Ключевые слова: защищённые сети передачи данных; маршрутизатор MikroTik; обновление программного обеспечения; механизмы аутентификации; сервисы и порты; межсетевое экранирование; скрипты.

USING MIKROTIK ROUTERS WHEN BUILDING SECURE DATA TRANSMISSION NETWORKS

Mandrick Dmitry, Sazonov Viktor
Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails: mandrick2013@yandex.ru, vmktor-sazonov@yandex.ru

Abstract. The use of MikroTik routers for testing the construction of secure data transmission networks will allow administrators to form an understanding of a number of security issues.

Keywords: secure data networks; MikroTik router; software updates; authentication mechanisms; services and ports; firewall; scripts.

В настоящее время процессы конвергенции, увеличение количества пользователей и процессы повышения качества предоставляемых услуг задают высокие темпы развития телекоммуникационных технологий. На ряду с гражданскими системами, так же идёт развитие и сетей передачи данных (СПД). Одним из основополагающих критериев, предъявляемых к СПД является безопасность, то есть состояние защищенности информации (сохранение ее в тайне и целостности), содержащейся в сообщениях при их передаче (приеме, обработке) в гетерогенных сетях [1-3].

Наряду со всем этим растут и требования к профессиональным компетенциям специалистов связи. В рамках их подготовки требуются большие затраты. Одним из вариантов решения данной задачи является использование общеизвестных аналогов, которые способны обладать схожими возможностями построения защищённой СПД, например, маршрутизатор MikroTik.

Известно [4-6], что маршрутизатор MikroTik является сравнительно безопасным роутером, обладающим высокой производительностью и широким набором функциональных возможностей. Однако, как и любое другое устройство, оно может быть уязвимо для различных видов атак, таких как атак на ssh, telnet или протоколы маршрутизации.

Важно отметить, что безопасность MikroTik в первую очередь зависит от уровня конфигурации, который был установлен на устройстве. Из-за богатого функционала и наличия множества настроек, неправильное конфигурирование может привести к серьезным уязвимостям.

Для обеспечения безопасности MikroTik следует придерживаться следующих рекомендаций:

– Регулярно обновлять программное обеспечение роутера;
– Настраивать механизмы аутентификации;
– Отключать неиспользуемые сервисы и порты;
– Использовать элементы межсетевого экранирования (запрещать прохождение нежелательных пакетов на определённых логических портах, фильтровать ненужные пакеты, подключаться к базам нежелательных доменных имен, анализировать трафик);
– Прописывать специальные скрипты, для работы в нестандартных условиях.

Соблюдение данных рекомендаций поможет обеспечить высокий уровень защищённости СПД. Однако, следует помнить, что в явном виде мы не сможем обеспечить стойкость защищённой СПД согласно требованиям руководящих документов.

СПИСОК ЛИТЕРАТУРЫ

1. Сытнюк А. А. Определение эффективного плана подготовки современных специалистов // Современные проблемы проектирования, производства и эксплуатации радиотехнических систем. 2016. № 10. С. 264-266.
2. Носов А. О., Житков А. П., Сазонов В. В., Файзулин В. В. Модель стационарной сети передачи данных // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020 г.: материалы конференции. Ч. 1. СПб: СПОИСУ, 2020. С. 95.
3. Сазонов В. В., Носов А. О. Моделирование сети передачи данных специального назначения // Перспективные направления развития отечественных технологий. V межрегиональная научно-практическая конференция: материалы конференции. Севастопольский государственный университет; Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации РАН. Севастополь, 2019. С. 212-214.
4. Житников Б. Ю., Ершова И. В., Блинов С. В. К вопросу о средствах защиты каналов связи в деятельности органов федеральной службы исполнения наказаний // III международный пенитенциарный форум «Преступление, наказание, исправление» : сб. тезисов выступлений и докладов участников Международной научно-практической конференции (Рязань, 21–23 ноября 2017 г.). Рязань: Академия ФСИН России, 2017. С. 287-292.
5. Рыжов Д. А., Курочкин Л. М., Глазунов В. В. Разработка методов аутентификации и защиты данных мобильных абонентов для доступа к облачным сервисам // Математические методы в технике и технологиях. ММТТ. 2020. Т. 10. С. 98-101
6. Яремчук С. MIKROTIK-ROUTER OS // Системный администратор. 2006. № 3 (40). С. 42-45.

УДК 621.391

КРИТЕРИИ ВЫБОРА ЭНЕРГОСБЕРЕГАЮЩЕГО МАРШРУТА ПЕРЕДАЧИ ДЛЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ С ВЫСОКОЙ ПЛОТНОСТЬЮ

Маслова Дарья Александровна
Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия
e-mail: dasha.kirilova.96@bk.ru

Аннотация. Беспроводные сенсорные сети (БСС) за последнее десятилетие обрели большую популярность и стали считаться одними из наиболее перспективных технологий беспроводной передачи данных. Области использования БСС значительно расширились, они используются не только для сбора, хранения и обработки информации, но и широко внедряются в различные сферы промышленности и в повседневную жизнь. В работе дается обобщенное определение понятия беспроводной сенсорной сети. Проводится анализ новых поколений связи. Предлагается энергосберегающий алгоритм выбора маршрута передачи пакета данных на базовую станцию. Положения предлагаемого алгоритма подтверждаются пространственно-энергетической моделью.

Ключевые слова: энергопотребление, беспроводная сенсорная сеть, пространственно-энергетическая модель, энергосберегающий алгоритм, плотность сети.

CRITERIA FOR SELECTING THE ENERGY SAVING ROUTE TRANSMISSIONS FOR HIGH DENSITY WIRELESS SENSOR NETWORKS

Maslova Daria
Nizhny Novgorod State of Engineering and Economic University
5 Oktyabrskaya St, Knyaginino, 606340, Russia
e-mail: dasha.kirilova.96@bk.ru

Abstract. Wireless sensor networks (WSNs) have gained great popularity over the past decade and have become one of the most promising technologies for wireless data transmission. The areas of use of WSNs have expanded significantly, they are used not only for collecting, storing and processing information, but are also widely introduced into various industries and into everyday life. The paper gives a generalized definition of the concept of a wireless sensor network. The analysis of new generations of communication is carried out. An energy-saving algorithm for choosing a route for transmitting a data packet to a base station is proposed. The provisions of the proposed algorithm are confirmed by the space-energy model.

Keywords: power consumption, wireless sensor network, spatial energy model, energy-saving algorithm, network density.

С каждым годом количество устройств, подключённых к сети, увеличивается, увеличивая тем самым плотность сети. Появляются новые поколения сете связи 5G, которое уже активно развивается в некоторых городах России, и планируемое направление дальнейшего развития сети шестого поколения. Последние сети получили так же название «сверхплотные сети», плотность устройств в таких сетях может составлять в среднем 100 устройств на 1 м2.

При данных условиях перед узлом источником ставится задача выбора маршрута передачи сообщения, затрачиваемого наименьшее количество энергии и удовлетворяющего времени доставки [2].

В работе предлагается алгоритм выбора маршрута передачи пакета данных на базовую станцию. Предполагается, что время доставки оценивается количеством ретрансляций на пути от узла-источника до базовой станции. Радиус действия передачи сигнала образует собой сектор. 2. В зависимости от удаленности узла-источника от базовой станции и радиуса дальности передачи сигнала определяется, сколько на маршруте будет секторов. Радиус сектора R может варьироваться в зависимости от параметра мощности передачи сенсорного узла.

По маршруту фиксируются опорные точки в виде начального и конечного узла сектора. На каждый сектор устанавливается допустимый предел мощности, которую можно потратить на передачу сообщения. Ретрансляция внутри сектора основана на следствии теоремы косинусов, предлагаемом ранее [3].

В работе предложена пространственно-энергетическая модель, позволяющая вычислить суммарное энергопотребление предлагаемого алгоритма. Проведен анализ показателей, полученных при расчетах пространственно-энергетической модели.

Таким образом, предлагаемый алгоритм выбора оптимального маршрута передачи пакета данных позволяет определить среди всех альтернативных путей передачи тот маршрут, который затрачивает наименьшее количество энергии.

СПИСОК ЛИТЕРАТУРЫ

1. Астахова Т. Н., Верзун Н. А., Касаткин В. В., Колбанев М. О., Шамин А. А. Исследование моделей связности сенсорных сетей // Информационно-управляющие системы, 2019. № 5. С. 38-50.
2. Оценка энергетических характеристик множественного доступа в эфирных сетях / Верзун Н. А. [и др.] // Известия СПбГЭТУ ЛЭТИ. 2019. № 10. С. 34-38.
3. Астахова, Т. Н., Кирилова, Д. А., Колбанёв, М. О., Маслов, Н. С., Шамин, А. А. Критерий выбора оптимального маршрута передачи сообщения в беспроводных сенсорных сетях // Телекоммуникации. 2020. № 7. С. 6-12.

УДК 621.396

АНАЛИЗ СПОСОБОВ СОЗДАНИЯ ПОГЛОЩАЮЩИХ ГРАНИЧНЫХ УСЛОВИЙ В МЕТОДЕ КОНЕЧНЫХ РАЗНОСТЕЙ ВО ВРЕМЕННОЙ ОБЛАСТИ

Мешалкин Валентин Андреевич, Шанин Александр Михайлович,
Коньков Денис Иванович, Ткачев Дмитрий Федорович
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: otesalex@yandex.ru, shanin.am@yandex.ru, den.konkov.94@mail.ru, dimas.portnoy@inbox.ru

Аннотация. Рассматриваются основные методы создания поглощающих граничных условий для решения задач электродинамики методом конечных разностей во временной области. Проводится анализ двух типов таких условий: аналитические и материальные. Подробно рассмотрены аналитические абсолютно поглощающие граничные условия Мура первого порядка.

Ключевые слова: методы усечения расчетного объема; метод конечных разностей во временной области; расчетная область; электромагнитное поле; численные методы.

ANALYSIS OF WAYS TO CREATE ABSORBING BOUNDARY CONDITIONS IN THE FINITE DIFFERENCE METHOD IN THE TIME DOMAIN

Meshalkin Valentin, Shanin Alexander, Konkov Denis, Tkachev Dmitry
Military Academy of Communications Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: otesalex@mail.ru, shanin.am@yandex.ru, den.konkov.94@mail.ru, dimas.portnoy@inbox.ru

Abstract. The main methods of creating absorbing boundary conditions for solving electrodynamics problems by the finite difference method in the time domain are considered. Two types of such conditions are analyzed: analytical and material. The analytical absolutely absorbing boundary conditions of Moore of the first order are considered in detail.

Keywords: methods of truncation of the calculated volume; the method of finite differences in the time domain; the calculated domain; electromagnetic field; numerical methods.

В соответствии с общим подходом решения задач электродинамики методом конечных разностей во временной области (КРВО) необходимо ограничить расчетную область, задав определённые соотношения на границе, обеспечивающие отсутствие отражений [1-4]. Иными словами, ограничение области есть, а граница прозрачна. Такие соотношения называются абсолютно поглощающими (абсорбирующими) граничными условиями (*absorbing boundary condition — ABC*).

Различают два типа таких условий: аналитические, сформулированные в виде математического соотношения (аналогичного условию излучения Зоммерфельда [5-7]), и материальные, использующие слои с комплексными электрофизическими параметрами.

Например, в аналитических АВС условиях Мура (*Mur*) электромагнитная волна не испытывает отражения в плоскости *x,* если для составляющей электрического поля при распространении волны на левую границу (в отрицательном направлении оси *x*) выполняется необходимое условие. Разложение в ряд Тейлора даёт необходимые соотношения. Таким же способом проводятся выводятся выражения и для правой границы. Условия такого типа называются аналитическими (математическими) граничными условиями *ABC*.

Если значения поля пространственных узлах временных узлах недоступны, применяют операцию усреднения. Далее получаем алгоритм для определения касательной компоненты в граничном узле. Такие условия называются аналитическими абсолютно поглощающими граничными условиями Мура первого порядка. Условие Мура справедливо только для волны, распространяющейся строго по нормали к границе и только для в дискретном случае [7-10], поэтому поверхность *ABC* должна располагаться на расстоянии, не меньшем половины длины волны от области решения.

В случае материальных АВС комплексные электрофизические параметры среды на границе подобраны таким образом, что можно создать неотражающий интерфейс. На границе задана искусственная среда с параметрами требуемыми макроскопическими параметрами [11, 12]. Падающая по нормали волна не отразится от границы раздела среда-свободное пространство, если их характеристические сопротивления равны. Так же необходимо сформулировать условия согласования.

Таким образом проведен анализ основных методов создания поглощающих граничных условий. Каждый из рассмотренных методов имеет свои особенности и специфику применения.

СПИСОК ЛИТЕРАТУРЫ

1. Григорьев А. Д. Методы вычислительной электродинамики. М., 2012. 432 с.
2. Липатников В. А., Парфиров В. А. Вероятностно-временные показатели процесса выявления сетей радиосвязи // Инновационные технологии и технические средства специального назначения. Труды XV научно-практической конференции В 2-х томах. СПб, 2023. Т. 1. С. 172-175.
3. Липатников В. А., Парфиров В. А. Вероятностно-временные характеристики процесса измерения координат робототехнических комплексов военного назначения по излучаемым радиосигналам // Перспективные системы и задачи управления. Материалы XVII Всероссийской научно-практической конференции и XIII молодёжной школы-семинара. Таганрог, 2022. С. 214-220.

4. Гладких Д. С., Парфиров В. А., Васильев Н. А. Математическая модель процесса обработки источников радиоизлучений комплексом радиоконтроля // Инновационные достижения и результаты научной деятельности операторов научных рот Вооруженных Сил Российской Федерации. Сборник научных статей по материалам круглого стола. Военная академия связи. СПб, 2022. С. 50-57.
5. Липатников В. А., Парфиров В. А. Способ повышения защищенности радиосигналов на основе стохастической модуляции // Технологии. Инновации. Связь. Материалы научно-практической конференции. СПб, 2023. С. 175-180.
6. Шанин А. М. Взаимное влияние элементов, защищенных активных фазированных антенных решёток // Теория и техника радиосвязи. Воронеж, 2022. № 4. С. 73-79.
7. Шанин А. М. Модель передающего радиоцентра на основе принципа электродинамического подобия // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. СПб, 2023. № 5-6(179-180). С. 71-78.
8. Мешалкин В. А., Чепелев К. В. Методика расчета внутренних характеристик активной фазированной антенной решетки с использованием современного программного обеспечения // Информационные системы и технологии. Орел, 2020. № 1(117). С. 89-96.
9. Мешалкин В. А., Викторов В. А., Пилюгин А. А. Проблема электромагнитной совместимости --- следствие научно-технического прогресса // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. М., 2019. № 12. С. 71-77.
10. Мешалкин В. А. Решение задач электродинамики с помощью вычислительного эксперимента // Прикладные информационные аспекты медицины. 2016. Т. 2. № 11. С. 80.
11. Лянгузов Д. А. Низкопрофильная антенна с изменяемой диаграммой направленности // Системы управления, связи и безопасности. СПб, 2022. № 2. С. 80-91.
12. Бородулин Р. Ю., Лянгузов Д. А. Модель низкопрофильной антенны для размещения на поверхности ограниченных размеров // Известия Тульского государственного университета. Технические науки. Тула, 2022. № 12. С. 193-199.

УДК 004.738

МЕТОДЫ МАРШРУТИЗАЦИИ ОДНОРАНГОВЫХ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

Миклуш Виктория Александровна
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mail: miklush-v@yandex.ru

Аннотация. Рассматриваются известные методы маршрутизации, применяемые при развертывании одноранговых беспроводных сенсорных сетей — простая, фиксированная и адаптивная. Обсуждаются особенности методов маршрутизации с учетом свойств беспроводных сенсорных сетей, таких как изменение топологии сети, ограничения вычислительных и энергетических ресурсов узлов сети.

Ключевые слова: беспроводная сенсорная сеть, маршрутизация, топология сети, ресурсы узла сети.

ROUTING METHODS FOR PED-UP WIRELESS SENSOR NETWORKS

Miklush Vuktoria
Saint Petersburg State University of Aerospace Instrumentation
67 Bolshaya Morskaya St, St. Petersburg, 190121 Russia
email: miklush-v@yandex.ru

Abstract. The well-known routing methods used in the deployment of peer-to-peer wireless sensor networks are considered — simple, fixed and adaptive. The features of routing methods are discussed considering the properties of wireless sensor networks, such as changes in the network topology, limitations of computing and energy resources of network nodes.

Keywords: wireless sensor network, routing, network topology, network node resources.

Известные методы маршрутизации в одноранговых беспроводных сенсорных сетях (БСС) — это простая, фиксированная и адаптивная маршрутизация, представленные несколькими вариантами реализации. Основное отличие между методами заключается в том, на сколько учитываются свойства БСС при выборе маршрута — изменение топологии сети, ограничения вычислительных и энергетических ресурсов узлов БСС [1-5].

В стратегии простой маршрутизации при выборе маршрута доставки данных не учитываются такие свойства БСС как возможное изменение топологии БСС и ограничения вычислительных и энергетических ресурсов узлов. Простая маршрутизация считается малоэффективной с точки зрения обеспечения кратчайшего пути и оптимального времени доставки данных, но обеспечивает гарантированную доставку данных в условиях потери узлов БСС. На практике распространение получили методы простой случайной маршрутизации и простой лавинной маршрутизации.

При реализации методов фиксированной маршрутизации для доставки данных будет выбран кратчайший путь с точки зрения числа хопов от узла-источника (И-узла) к узлу-адресату (А-узлу), но без учета расхода вычислительных и энергетических ресурсов транзитных узлов (Т-узлов). Для каждой пары источник-адресат в узле-координаторе строится кратчайший путь в соответствии с актуальной таблицей маршрутизации. Таблица маршрутизации также хранится в узле-координаторе и обновляется при изменении топологии БСС, правда с задержкой, задаваемой временем опроса всех узлов. Отсутствие учета расхода вычислительных и энергетических ресурсов Т-узлов при выборе маршрута приводит к тому, что одни и те же Т-узлы будут выбраны в качестве ретрансляторов данных, что чревато возникновениями коллизий при доступе к ресурсам Т-узлов, потерями данных и неоправданными задержками доставки данных.

Методы адаптивной маршрутизации учитывают изменение топологии БСС и нагрузку на ее узлы. Все существующие варианты адаптивной маршрутизации различаются только показателями, учитываемыми при выборе маршрута.

СПИСОК ЛИТЕРАТУРЫ

1. Миклуш В. А., Татарникова Т. М. Имитационная модель одноранговой беспроводной сенсорной сети // T_Comm: Телекоммуникации и транспорт. 2023. Т. 17, № 3. С. 20-21.
2. Kraeva E., Miklush V., Palkin I., Tatarnikova T., Kunturov A. Information support in environmental monitoring systems // IOP Conference Series: Earth and Environmental Science. Сер. All-Russian Scientific-Technical Conference «Digital Technologies in Forest Sector». 2020. Vol. 507. Pp. 012-015.
3. Татарникова Т. М., Елизаров М. А. Процедура разрешения коллизий в RFID-системе // Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 2. С. 150-157.
4. Татарникова Т. М. Статистические методы исследования сетевого трафика // Информационно-управляющие системы. 2018. № 5(96). С. 35-43.
5. Татарникова Т. М., Миклуш В. А., Рудых С. В. Оценка показателей качества обслуживания беспроводных сенсорных сетей // Информация и Космос. 2022. № 4. С. 21-27.

УДК 621.396.4

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ТЕХНИЧЕСКАЯ НАДЕЖНОСТЬ МОБИЛЬНЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ: ПОДХОД К ФОРМИРОВАНИЮ ПОКАЗАТЕЛЕЙ ДЛЯ ТЕКУЩЕГО И ПРОАКТИВНОГО КОНТРОЛЯ

Михайличенко Антон Валерьевич, Паращук Игорь Борисович, Селезнев Андрей Васильевич
Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: toni09_91@mail.ru, shchuk@rambler.ru, andrsel@mail.ru

Аннотация. В докладе рассматривается задача построения и корректной математической формулировки вероятностного комплексного показателя информационной безопасности и технической надежности мобильных центров обработки данных. Данный комплексный показатель призван обеспечить текущий и проактивный контроль информационной безопасности и надежности систем такого класса, он создан на основе совместной условной вероятности выполнения требований к отклонениям частных показателей безопасности и надежности. Исследованы подходы к формулировке частных показателей информационной безопасности и технической надежности, изучены перспективные направления для создания на их основе алгоритмов точного и своевременного текущего и проактивного контроля безопасности и надежности современных мобильных центров обработки данных.

Ключевые слова: мобильный центр обработки данных, информационная безопасность, показатель технической надежности, проактивный контроль, требования, условная вероятность, ремонтопригодность.

INFORMATION SECURITY AND TECHNICAL RELIABILITY OF MOBILE DATA CENTERS: AN APPROACH TO THE FORMATION OF INDICATORS FOR CURRENT AND PROACTIVE CONTROL

Mikhailichenko Anton, Parashchuk Igor, Seleznev Andrey
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: toni09_91@mail.ru, shchuk@rambler.ru, andrsel@mail.ru

Abstract. The report considers the problem of constructing and correct mathematical formulation of a probabilistic complex indicator of information security and technical reliability of mobile data centers. This complex indicator is designed to provide current and proactive control of information security and reliability of systems of this class, it is created on the basis of a joint conditional probability of meeting the requirements for deviations of particular indicators of security and reliability. Approaches to the formulation of particular indicators of information security and technical reliability are investigated, promising directions for creating algorithms based on them for accurate and timely current and proactive control of the security and reliability of modern mobile data centers are studied.

Keywords: mobile data center, information security, technical reliability indicator, proactive control, requirements, conditional probability, maintainability.

Анализ исследований в области контроля и управления современными мобильными центрами обработки данных (МЦОД) показывает, что сравнительная вероятностно-временная и многокритериальная оценка технической надежности таких сложных информационно-технических объектов непосредственно по частным показателям не только мало информативна, почти не применима в реальной практике, но и, зачастую, противоречива.

Мобильные центры обработки данных являются полноценными одномодульными аналогами классических центров обработки данных, но размещаются либо в специальном боксе на транспортной базе (автомобиль, судно, самолет), либо в специализированном транспортном контейнере (для перевозки железнодорожным, автомобильным или водным транспортом).

Сложность сравнительной вероятностно-временной и многокритериальной оценки технической надежности таких сложных информационно-технических объектов связана с тем, что по одним показателям более надежным может оказаться один МЦОД, а по другим — совсем другой мобильный дата-центр, с другим или даже с таким же набором элементов — средств и комплексов связи, хранения и обработки данных [1-3].

Этот объективный факт, затрудняющий оценку и связанный с многообразием и разноплановостью анализируемых и подлежащих текущему и проактивному контролю аспектов и показателей надежности технических (аппаратно-программных) систем, присутствует, несмотря на то, что существует целый ряд международных и национальных стандартов, определяющих не только методологические подходы к анализу надежности систем такого класса, но и примерный перечень параметров, по которым она могут быть оценена в целом, либо могут быть отдельно оценены такие аспекты технической надежности, как безотказность, долговечность, ремонтопригодность и сохраняемость [4, 5].

Помимо этого, приходится также учитывать субъективизм формулировки некоторых частных показателей технической надежности (ЧПТН), вносящий известную долю неопределенности в решение задач управления и вероятностно-временного оценивания безотказности, долговечности, ремонтопригодности и сохраняемости современных МЦОД [6, 7].

Выход из этой ситуации нам видится в формулировке и последующей текущей либо прогностической оценке вероятностного комплексного показателя технической надежности (КПТН) МЦОД, который бы функционально связывал все многообразие ЧПТН и требований к ним.

Анализ различных методов формирования комплексных (обобщенных) показателей качества, надежности либо эффективности сложных систем показал, что наиболее полный учет особенностей решения задачи оценивания технической надежности МЦОД, а также естественное решение проблем нормализации и свертки систем показателей технической надежности (ПТН) достигается при применении метода вероятностной скаляризации [8, 9].

Сущность данного метода состоит в использовании в качестве КПТН совокупной (совместной) вероятности выполнения требований, предъявляемых пользователем к технической надежности мобильного дата-центра на каждом шаге его эксплуатации по безотказности, долговечности, ремонтопригодности и сохраняемости.

Предпочтение, отданное данному методу, обусловлено учетом в нем случайного характера изменений основной массы ПТН МЦОД, а также практической возможностью автоматического решения основных проблем многокритериальной вероятностно-временной оценки качества, надежности и эффективности функционирования сложных технических систем (т.е., в нашем случае, возможностью нормализации компонент векторных ПТН МЦОД и их свертки) в рамках выбранного вероятностного подхода к анализу технической надежности [9].

Фундамент данного метода основан на пошаговом (поэтапном) расчете ЧПТН на любом шаге оценивания и их математически корректной «свертке» в КПТН МЦОД на этом же шаге. Математически метод может быть осуществлен на основе аппарата условных вероятностей, а также классических теорем функциональной и параметрической декомпозиции [9].

При этом вероятностный комплексный ПТН формируется из условных вероятностей выполнения требований к отклонениям ЧПТН МЦОД. Иными словами, для методики, учитывающей вероятностно-временную физическую сущность трансформации ПТН МЦОД на каждом шаге его эксплуатации и, учитывая тот факт, что ПТН представляют собой отклонения параметров надежности от требуемых значений, КПТН, может быть аналитически записан как совместная условная вероятность выполнения требований к значениям отклонений показателей безотказности, долговечности, ремонтопригодности и сохраняемости МЦОД.

При этом вариант формулировки отдельного вероятностного частного ПТН, характеризующего, например, такой аспект (грань) надежности МЦОД, как безотказность, может быть представлен в виде условной вероятности выполнения требований на каждом шаге эксплуатации МЦОД к отклонениям значений вероятности безотказной работы, средней наработки до отказа, средней наработки на отказ и интенсивности потока отказов, рассчитываемой при условии выполнения требований, например, к отклонениям одного из ключевых параметров безотказности — средней доли безотказной наработки.

Аналогичные показатели могут быть сформулированы и для информационной безопасности МЦОД.

Таким образом, можно с большой долей уверенности утверждать, что, с учетом оговоренных ограничений на множество ПТН, формулировка вероятностного комплексного ПТН может быть осуществлена на основе условных вероятностей выполнения требований к отклонениям частных показателей надежности МЦОД, характеризующих параметры его безотказности, долговечности, ремонтопригодности и сохраняемости. Предложен вариант формулировки ЧПТН, включающий условную вероятностную меру выполнения требований к отклонениям частных параметров безотказности.

Рассмотренный подход обладают универсальностью, а сочетание метода вероятностной скаляризации и математического аппарата условных вероятностей обуславливает перспективы в вопросах достоверного и оперативного проактивного контроля информационной безопасности и надежности современных мобильных центров такого класса.

СПИСОК ЛИТЕРАТУРЫ

1. Андреев А. В. Яковлев В. В., Короткая Т. Ю. Теоретические основы надежности технических систем : учеб. пособие. СПб : Изд. Полит. ун-та, 2018. 164 с.
2. Изергина А. Р. Обзор статистических методов оценки надежности // Математические модели современных экономических процессов,

методы анализа и синтеза экономических механизмов. Актуальные проблемы и перспективы менеджмента организаций в России : сб. ст. XII Всерос. науч.-практ. конф. Самара : Изд-во СамНЦ РАН, 2018. С. 45-50.
3. Паращук И. Б., Михайличенко Н. В., Михайличенко А. В. Нейро-нечеткие сети и алгоритмы гранулярных вычислений в задачах интеллектуальной обработки данных для оценки надежности мобильных дата-центров // Применение искусственного интеллекта в информационно-телекоммуникационных системах : сб. материалов научно-практической конференции. СПб : ВАС, 2021. С. 110-115.
4. Межгосударственный стандарт ГОСТ 27.002-2015 Надежность в технике. Термины и определения. М. : Стандартинформ., 2016. 30 с.
5. Национальный стандарт РФ ГОСТ Р 51901.5-2005 (МЭК 60300-3-1:2003) Менеджмент риска. Руководство по применению методов анализа надежности. М. : Стандартинформ., 2005. 44 с.
6. Паращук И. Б., Михайличенко А. В., Крюкова Е. С. Анализ зашумленных и неоднородных данных о значениях параметров надежности дата-центров // Современные технологии: актуальные вопросы теории и практики : сб. статей Международной НПК. Пенза : МЦНС «Наука и Просвещение», 2021. С. 74-77.
7. Паращук И. Б., Башкирцев А. С., Михайличенко Н. В. Анализ уровней и видов неопределенности, влияющей на принятие решений по управлению информационными системами // Информация и космос. № 1, 2017. С. 112-120.
8. Надежность и эффективность в технике. Т. 3. Эффективность технических систем. / под ред. В. Ф. Уткина и Ю. В. Крючкова. М. : Машиностроение, 1988. 328 с.
9. Терентьев В. М., Санин Ю. В. Анализ эффективности функционирования автоматизированных сетей многоканальной радиосвязи. СПб : ВАС, 1992. 80 с.

УДК 004.056

АНАЛИЗ ПРИМЕНЕНИЯ ЭЛЕМЕНТОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ТЕХНИЧЕСКОГО ВУЗА

Мнацаканян Владислав Анатольевич[1], Новосёлов Сергей Витальевич[1], Пантюхин Олег Игоревич[2]
[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
[2] Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: vladgc7@gmail.com, novosyosergej@yandex.ru, p_oleg99@mail.ru

Аннотация. В докладе представлены результаты исследования решений, обеспечивающих возможность внедрения элементов искусственного интеллекта на основе обновления программ обучения технических высших учебных заведений. Приведены примеры по успешному внедрению искусственного интеллекта в сферу образования.

Ключевые слова: искусственный интеллект; программы обучения технического университета; развитие сферы образования.

ANALYSIS OF APPLICATION OF ELEMENTS OF ARTIFICIAL INTELLIGENCE IN THE EDUCATIONAL ACTIVITY OF A TECHNICAL UNIVERSITY

Mnatsakanyan Vladislav[1], Novoselov Sergey[1], Pantyukhin Oleg[2]
[1] The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
22 Bol'shevikov Av., k.1, St. Petersburg, 193232, Russia
[2] The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails: vladgc7@gmail.com, novosyosergej@yandex.ru, p_oleg99@mail.ru

Abstract. The expected results of the research contain the possibility of introducing elements of artificial intelligence based on updating the software of the higher technical technology of universities. Examples of the successful implementation of artificial intelligence in the field of education are given.

Keywords: artificial intelligence; training programs of a technical university; development of the education sector.

На сегодняшний день технологии искусственного интеллекта (ИИ) активно проникают во все сферы человеческой деятельности. В этом контексте стоит отметить, что Президент Российской Федерации в своем Указе от 10 октября 2019 года, под названием «О развитии искусственного интеллекта в Российской Федерации», утвердил Национальную стратегию развития ИИ на период до 2030 года. Этот документ обозначает приоритетность развития ИИ в стране и его значимость для достижения стратегических целей.

Кроме того, правительство РФ получило задание разработать и утвердить федеральный проект «Искусственный интеллект» и внести соответствующие изменения в национальную программу «Цифровая экономика Российской Федерации». Этот шаг направлен на поддержку и развитие исследований, инноваций и внедрения ИИ в различных сферах, включая образование, здравоохранение, промышленность и другие [1, 2].

Такие инициативы и указания государственных органов свидетельствуют о признании значимости ИИ и его потенциала для развития страны. Внедрение ИИ может повысить эффективность и результативность многих процессов, способствуя прогрессу и инновациям. Реализация Национальной стратегии и федерального проекта позволит создать благоприятные условия для развития ИИ, привлечения высококвалифицированных специалистов и стимулирования инвестиций в эту область [1, 2].

Внедрение ИИ в сферу высшего образования представляет собой необходимость, обусловленную рядом факторов и потенциальных выгод [3]. В настоящее время разрабатываются новые образовательные программы, например, «Искусственный интеллект в сетях и системах связи», «Искусственный интеллект в сетях связи»,

«Теоретические основы построения систем искусственного интеллекта» и другие. В докладе представлены научно-обоснованные аргументы о целесообразности использования ИИ в технических ВУЗах.

Применение ИИ в высшем образовании может обеспечить персонализацию образовательного процесса. Системы ИИ способны анализировать множество данных о студентах, таких как предпочтения, академические достижения, образовательные потребности и индивидуальные особенности. На основе этого анализа можно создавать индивидуальные программы обучения, предоставлять персонализированные материалы и методики обучения, что повысит эффективность образовательного процесса и удовлетворит потребности студентов.

В настоящее время для студентов ВУЗов доступно множество научно-образовательных платформ в сети Интернет, которые с использованием технологий ИИ позволяют искать, отбирать и анализировать информацию. Для ВУЗов необходима оценка публикуемого контента для субъектов образовательно процесса, требуется изучать возможные системы отслеживания и анализа цифровых онлайн-платформ (научно-образовательных сайтов) [4]. При этом важно анализировать получаемые сведения, имея в виду, что они могут быть ошибочными или даже заведомо ложными. Борьба с неверной информацией может вестись путем сопоставления информации из разных источников, анализа и ранжирования информации по степени доверия к ней.

ИИ позволяет также автоматизировать административные задачи в сфере высшего образования. Автоматизация рутинных задач освободит преподавателей и администрацию от монотонной работы и позволит им сконцентрироваться на более творческих и стратегических аспектах образовательного процесса. Внедрение ИИ может обеспечить быструю и точную проверку текущих контрольных и экзаменационных работ, а также предоставлять студентам обратную связь с преподавателями и администрацией ВУЗа [3].

Кроме того, системы ИИ могут предлагать рекомендации и советы по улучшению знаний, умений и навыков на основе анализа работы студентов, что поможет им эффективнее учиться и прогрессировать. ИИ предоставляет возможности для инноваций в методах обучения. Например, использование виртуальной реальности и симуляций предоставит студентам возможности получения новых и развития имеющихся практических навыков.

Один из научных примеров программ ИИ в высшем образовании — это системы интеллектуального тьюторства. Такие программы используются для поддержки и улучшения образовательного процесса, предоставляя студентам персонализированное обучение и обратную связь.

Например, проект Cognitive Tutor, разработанный учеными из Карнеги-Меллонского университета, представляет собой программу ИИ, которая помогает студентам в изучении математики. Система анализирует ответы студентов на задачи, определяет их уровень понимания и предлагает индивидуальные рекомендации и объяснения. Она также адаптируется к учебным потребностям студентов и корректирует свои предложения в зависимости от их прогресса и трудностей [4].

Другим примером является проект Watson, разработанный компанией IBM. В рамках высшего образования, система Watson может использоваться для анализа и обработки больших объемов информации, например, научных статей и публикаций. Система может выявлять связи и тенденции в исследованиях, помогать студентам и преподавателям проводить литературный обзор, исследовать новые области и получать более полное представление о состоянии научных знаний [5, 6].

Такие программы ИИ в высшем образовании позволяют студентам получать индивидуализированное обучение и поддержку, а также помогают преподавателям оптимизировать процесс обучения и предоставлять более эффективную обратную связь. Подведем итоги анализа направлений применения элементов ИИ — это:

1) персонализация образования: ИИ может анализировать данные о студентах, их учебных предпочтениях и способностях для предоставления персонализированных учебных материалов и методик обучения. Это позволяет студентам учиться в своем собственном темпе и сосредоточиться на наиболее релевантных для них темах;

2) автоматизация административных задач: ИИ может автоматизировать рутинные административные задачи, такие как проверка и оценка работ студентов, составление расписания занятий и ответы на стандартные вопросы студентов. Это позволяет преподавателям и администрации университета сосредоточиться на более творческих и стратегических задачах;

3) улучшение обратной связи: ИИ может помочь улучшить обратную связь для студентов. Например, он может предлагать рекомендации по улучшению академических навыков на основе анализа производительности студента. Также ИИ может обеспечить быструю и точную проверку заданий и экзаменов, предоставляя студентам немедленную обратную связь;

4) инновации в методах обучения: ИИ может предложить новые методы обучения, основанные на анализе данных и прогнозировании тенденций. Например, использование виртуальной реальности и симуляций может помочь студентам получить практические навыки в реалистичной среде. Это позволяет создать более интерактивную и захватывающую обучающую среду;

5) исследования и аналитика: ИИ может использоваться для обработки больших объемов данных и проведения анализа для исследований в области высшего образования. Он может помочь выявить тенденции и наиболее лучшие методики (паттерны), улучшить предсказательную аналитику и оптимизировать принятие решений в техническом университете.

Искусственный интеллект в сфере образования демонстрирует значимый потенциал. Он позволяет предоставлять персонализированное обучение на основе анализа данных о студентах. Использование ИИ также улучшает обработку больших объемов информации и обеспечивает более глубокий анализ данных. Однако,

внедрение ИИ в образование сталкивается с вызовами, такими как опасения замены традиционных методов обучения. Баланс между ИИ и человеческим взаимодействием является важным аспектом этого процесса.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».
2. Президиум прав комиссии по цифровому развитию утвердил федеральный проект «Искусственный интеллект» // Digital Russia, 31.08.2020.
3. Пантюхин О. И., Рябов Г. А., Солодухин Б. В., Юдин А. А. Перспективные направления использования искусственного интеллекта в образовании // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021) : сборник научных статей : в 4-х т. Санкт-Петербург, 2021. С. 279-284.
4. Технологии искусственного интеллекта в программных системах мониторинга научно-образовательных сайтов в сети интернет / Г. А. Рябов, О. И. Пантюхин [и др.] // Тенденции развития науки и образования. 2023. № 93-2. С. 103-107.
5. Искусственный интеллект в образовании // TAdviser [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/ (дата обращения: 30.06.2023).
6. IBM Watson // TAdviser [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Продукт: IBM_Watson (дата обращения: 30.06.2023).

УДК 621.391

ПОДХОД К ПОСТРОЕНИЮ МОДЕЛИ СЛОЖНОЙ ТЕХНИЧЕСКОЙ СИСТЕМЫ

Остроумов Олег Александрович, Лепешкин Олег Михайлович,
Синюк Александр Демьянович, Ренсков Дмитрий Андреевич
Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: oleg-26stav@mail.ru, lepechkin1@yandex.ru, eentrop@yandex.ru

Аннотация. В докладе представлен подход к моделированию сложных технических систем, предлагается строить модель, состоящую из структурной и функциональных характеристик системы, связанных через матрицу ресурсов системы.

Ключевые слова: сложная техническая система, функциональная устойчивость, модель, функции, задачи.

APPROACH TO BUILDING A COMPLEX TECHNICAL SYSTEM MODEL

Ostroumov Oleg, Leptchkin Oleg, Sinyk Aleksander, RenskovDmitrii
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Pr, St. Petersburg, 194064, Russia
e-mails: oleg-26stav@mail.ru, lepechkin1@yandex.ru, eentrop@yandex.ru

Abstract. The report presents an approach to modeling complex technical systems, it is proposed to build a model consisting of the structural and functional characteristics of the system, linked through the system resource matrix.

Keywords: complex technical system, functional stability, model, functions, tasks.

Большинство современных технических систем являются сложными. Сложность таких систем обусловлена количеством элементов, входящих в нее, а также возможностями по выполнению функций и задач. Сложные технические системы сложно формализуемы, по причине необходимости учета множества связей между их элементами. Наряду с этим для таких систем, из-за большого количества процессов, происходящих в них необходим постоянный контроль функционирования системы. Знание состояния системы и ее элементов в любой момент времени позволит обеспечить выполнение системой требуемого перечня функций и задач [1, 2]. Для описания функционирования требуется формализация и моделирование системы, которые бы позволили выявлять и в последующем устранять нарушения функционирования системы. При моделировании различных систем, как правило, рассматривают структур системы [3-7]. Структурная модель представляет собой граф, включающий элементы системы и связи между ними. В работе предлагается модель системы, включающая не только структурную характеристику системы, но и функциональную. Отличительной особенностью предлагаемой модели является то, что она позволяет оценивать не только структурную составляющую процесса функционирование СС, но и функциональную устойчивость самой системы, т.е. способности системы выполнить требуемый объем задач и функций системы, при этом обеспечение функциональной устойчивости возможно в условиях устойчивого функционирования системы управления системы, реализованной через обратную связь реакции системы управления на происходящие изменения состояния системы связи под действием различных факторов

Цель работы — разработка графо-матричной структурно-функциональной модели сложной технической системы, позволяющей оценивать возможности существующей системы связи или ее элементов по обеспечению процесса управления через количественную оценку выполнения ее задач и функций. Модель представляет собой совокупность матриц, описывающих структуру и функциональные возможности системы и ее элементов [8]:

характеризующих структуру системы:

матрица $\boldsymbol{Y_X}=\{y_{X,j}\}_{XxX}$ смежности, включающая признаки наличия узловых и линейных сетевых элементов, соединяющих вершины графа (узлы) $i,j\in[1,X]$, где X — общее количество вершин (узлов) в системе;

матрица $\boldsymbol{Y_{пс}}=\{y_{пci,j}\}_{XxX}$ и вектор $\boldsymbol{cN}=\{cX_k\}_K$ пропускных способностей сетевых элементов;

матрица $\boldsymbol{Y_г}=\{y_{гi,j}\}_{XxX}$ и вектор $\boldsymbol{pN}=\{cX_k\}_K$ коэффициентов готовности сетевых элементов;

матрица $\boldsymbol{Y}_{\text{вк}}=\{y_{\text{вк}i,j}, y_{\text{вк}i,j}\}_{XxX}$ весовых коэффициентов узлов и линий связи;

матрица $\boldsymbol{Y}_{\text{ип}}=\{y_{\text{ип}i,j}\}_{XxX}$ информационных потоков между узлами системы в единицах требуемой пропускной способности для обеспечения требуемого качества обслуживания;

матрица $\boldsymbol{Y}_{\text{тп}}=\{y_{\text{тп}i,j}\}_{XxX}$ технологических потоков между узлами системы;

матрица $\boldsymbol{Y}_{\text{пип}}=\{y_{\text{пип}i,j}\}_{XxX}$ приоритетов информационных потоков между узлами системы;

матрица $\boldsymbol{Y}_{\text{птп}}=\{y_{\text{птп}i,j}\}_{XxX}$ приоритетов информационных потоков между узлами системы;

характеризующих функционирование системы:

матрица $\boldsymbol{Y}_{\boldsymbol{E}}=\{y_{Ei,j}\}$ задействования ресурсов системы;

матрица $\boldsymbol{Y}_{\boldsymbol{Z}}=\{y_{Zi,j}\}$ выполнения задач системы;

матрица $\boldsymbol{Y}_{\boldsymbol{F}}=\{y_{Fi,j}\}$ выполнения функций системы;

матрица $\boldsymbol{Y}_{\boldsymbol{T}}=\{y_{Ti,j}\}$ требований, предъявляемых к системе и ее элементам;

матрица $\boldsymbol{Y}_{\boldsymbol{A}}=\{y_{Ai,j}\}$ выполнения целей системы;

матрица $\boldsymbol{Y}_{\boldsymbol{X\text{-}E}}=\{y_{i,j}\}$ предоставления ресурсов, включающая ресурсы, которые предоставляют узлы и линии связи системы;

матрица $\boldsymbol{Y}_{\boldsymbol{Z\text{-}E}}=\{y_{Zi,j}\}$ выполнения задач, включающая ресурсы задействованные для выполнения каждой задачи;

матрица $\boldsymbol{Y}_{\boldsymbol{F\text{-}Z}}=\{y_{Fi,j}\}$ выполнения функций, включающей функции и задачи, выполнение которых позволит выполнить каждую функцию;

матрица $\boldsymbol{Y}_{\boldsymbol{A\text{-}F}}=\{y_{Ai,j}\}$ выполнения целей, включающая цели и функции, выполнение которых позволит выполнить каждую цель;

матрица $\boldsymbol{Y}_{\boldsymbol{E\text{-}T}}=\{y_{Ei,j}\}$ соответствия ресурсов, предъявляемым к ним требованиям;

матрица $\boldsymbol{Y}_{\boldsymbol{Z\text{-}T}}=\{y_{Zi,j}\}$ соответствия задач, предъявляемым к ним требованиям;

матрица $\boldsymbol{Y}_{\boldsymbol{F\text{-}T}}=\{y_{Fi,j}$ соответствия функций, предъявляемым к ним требованиям;

матрица $\boldsymbol{Y}_{\boldsymbol{A\text{-}T}}=\{y_{Ai,j}\}$ соответствия целей, предъявляемым к ним требованиям.

Таким образом предлагаемая модель сложной технической системы позволяет оценивать возможности системы по выполнению функций и задач. Способность системы их выполнять будет характеризоваться ее функциональной устойчивостью. Знание функциональной устойчивости и состояния системы в любой момент времени позволит своевременно и качественно реагировать на изменения в системе и окружающем мире, а также обеспечить требуемый уровень функциональной устойчивости системы.

СПИСОК ЛИТЕРАТУРЫ

1. Лепешкин О. М. Синтез модели процесса управления социальными и экономическими системами на основе теории радикалов: специальность 05.13.10 «Управление в социальных и экономических системах»: дис. … д-р тех. наук. СПб: Санкт-Петербургский политехнический университет Петра Великого, 2014. 428 с.
2. Остроумов О. А. Проблема обеспечения функциональной устойчивости систем критически важных объектов. Электросвязь. 2022. № 1. С. 14-18.
3. Исаков Е. Е. Устойчивость военной связи в условиях информационного противоборства. СПб.: Политехнический университет, 2009. 400 с.
4. Иванов В. Г. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи : монография. СПб.: ПОЛИТЕХ-ПРЕСС, 2018. 214 с.
5. Kotenko I., Saenko I., Lauta O., Kribel K. An approach to modeling of the security system of intelligent transport systems based on the use of flat graphs // Lecture Notes in Networks and Systems (LNNS). 2021. Vol. 330. P. 440-451.
6. Беляков М. И. Модель процесса функционирования системы обеспечения информационной безопасности объекта критической информационной инфраструктуры в задаче оценивания его эффективности // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму, 2020. № 11-12 (149-150). С. 71–75.
7. Одоевский С. М., Лебедев П. В. Методика оценки устойчивости функционирования системы технологического управления инфокоммуникационной сетью специального назначения с заданной топологической и функциональной структурой // Системы управления, связи и безопасности. 2021. № 1. С. 152-189. DOI: 10.24411/2410-9916-2021-10107.
8. Остроумов О. А. Методика обеспечения функциональной устойчивости системы связи // Вопросы радиоэлектроники. Серия: Техника телевидения, 2022. Вып. 1. С. 30-38.

УДК 621.391

ПРОФИЛЬ ФУНКЦИОНИРОВАНИЯ СЛОЖНОЙ ТЕХНИЧЕСКОЙ СИСТЕМЫ

Перов Роман Александрович, Остроумов Олег Александрович, Филимонов Василий Александрович

Военная академия связи им. Маршала Советского Союза С. М. Буденного,

Тихорецкий пр., 3, Санкт-Петербург, Россия

e-mail: oleg-26stav@mail.ru, roma.perov@list.ru, awgn@yandex.ru,

Аннотация. В докладе рассмотрен подход формализации процесса функционирования сложной технической системы через профиль ее функционирования, представляющий собой набор характеристик, правил, описывающих процесс функционирования системы.

Ключевые слова: функциональная устойчивость, критичность, система связи, система управления, сложная техническая система, функции, задачи, профиль, регламент.

FUNCTIONING PROFILE OF A COMPLEX TECHNICAL SYSTEM

Perov Roman, Ostroumov Oleg, Filimonov Vasily

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,

3 Tikhoretsky Av. St., Petersburg, Russia

e-mails: oleg-26stav@mail.ru, roma.perov@list.ru, awgn@yandex.ru

Abstract. The report considers the approach of formalizing the process of a complex technical system functioning process through the profile of its functioning, which is a set of characteristics, rules that describe the system functioning process.

Keywords: functional stability, criticality, communication system, control system, complex technical system, functions, tasks, profile, regulations.

Количество сложных технических систем (СТС) с каждым годом увеличивается. Это связано с развитием технологий, появлением новых функций, элементов в таких системах, а также оптимизацией процесса управления одной или несколькими системами. В процессе функционирования такие системы предоставляют различные услуги пользователям, решают задачи и выполняют функции. Нарушение функционирования таких систем становится критичным для их пользователей, возникает проблема обеспечения функциональной устойчивости таких систем. Под функциональной устойчивостью сложной технической системы будет пониматься способность системы выполнять требуемый перечень функций и задач с требуемым качеством и установленные сроки. Критичность элементов системы и ее самой может меняться в зависимости от необходимости их использования в процессе функционирования системы, поэтому можно различать статическую и динамическую критичность [1, 2].

Критичность — свойство объекта, системы, элемента характеризующее последствия нарушения его (ее) устойчивого функционирования, которое может привести к потере управления, нанести ущерб жизни и здоровью граждан, интересам организации, государства, окружающей среде, безопасности, обороноспособности государства, а также привести к другим тяжелым последствиям.

Динамическая критичность — критичность, изменяемая во времени, в зависимости от выполняемых задач и функций объекта, условий в которых он функционирует.

Статическая критичность — критичность объекта, системы, элемента присущие им постоянно.

Для формализации системы, позволяющей выявлять критичность тех или иных ее элементов, а также для контроля ее функционирования и обеспечения ее устойчивого функционирования предлагается разработать профиль функционирования системы. Необходимость разработки такого инструмента также обусловлена сложностью формализации СТС [3, 4].

Под профилем системы будем понимать набор взаимосвязанных характеристик, правил построения системы, описывающих процесс функционирования СТС на заданном отрезке времени с требуемыми ограничениями [5].

Цель исследования заключается в разработке подхода к формализации СТС и формировании профиля системы, характеризующего сложную техническую систему, процессы и регламенты, происходящие в ней, являющегося инструментом системы контроля, который позволяет выявлять и своевременно реагировать на отклонения от устойчивого функционирования системы.

Предложенный подход к описанию функционирования системы через формирование профиля функционирования системы включает следующие этапы:

На первом этапе строится графо-матричная структурно-функциональная модель системы связи, представляющая собой граф характеризующий структуру системы связи, который описывается матрицами. Структурная модель системы связи предоставляет определенный ресурс для выполнения задач системы, функциональная модель, представляющая собой зависимые ресурсы, задачи, функции, цели и требования строится на основе структурной модели и описывается матрицами функционирования. Результатом построения модели является совокупность взаимосвязанных и взаимовложенных матриц, описывающих структуру системы связи и выполняемые ее задачи, функции, цели и требования.

На втором этапе на основании графо-матричной структурно-функциональной модели строятся одиночные профили СС, описывающие задачи и функции системы, для выполнения которых используется только один элемент системы (задача, ресурс). Результатом построения одиночных профилей является совокупность матриц, описывающих задачи и функции системы связи.

На третьем этапе формируются групповые профили системы связи, представляющие собой совокупности одиночных и групповых профилей системы, представленные в виде матриц и характеризующих выполнение системой функций, целей, требований. Формируется три типа групповых профилей: состоящие только из одиночных профилей и состоящий только из групповых профилей, состоящий из одиночных и групповых профилей.

На четвертом этапе осуществляется согласование одиночных и групповых профилей по влиянию друг на друга и времени выполнения.

Таким образом предложен подход к описанию функционирования системы связи через формирование профиля функционирования системы, представляющий собой совокупность матриц, который используется в системе контроля. Основным отличие представленного подхода от известных [6-10] является формализация процесса функционирования системы, определение его зависимости, через ресурс, от структуры системы, и представление системы в виде профиля функционирования системы, позволяющего количественно определять возможности системы по выполнению функций, задач и целей, а также осуществлять синтез системы для выполнения ее целевого предназначения. Результаты исследования могут быть использованы при проектировании и построении сложных технических систем, систем контроля, диагностики и мониторинга состояния системы.

СПИСОК ЛИТЕРАТУРЫ

1. Остроумов О. А. Методология обеспечения процесса устойчивого функционирования системы связи — критически важного объекта системы управления // Военная мысль. 2022. № 9. С. 52-58.
2. Lepeshkin O. M., Ostroumov O. A., Sinyuk A. D. The communication system functional stability with critical objects // Проблемы управления безопасностью сложных систем. Материалы XXIX международной научно-практической конференции. Москва, 2021. С. 80-85.
3. Ранжирование объектов критической информационной инфраструктуры системы связи / О. М. Лепешкин [и др.] // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021) : сборник статей X Международной научно-технической и научно-методической конференции. Санкт-Петербург, 2021. С. 289-295.
4. Лепешкин О. М., Синюк А. Д., Карпов М. А., Остроумов О. А. Методологический подход управления обеспечением функциональной безопасности и функциональной устойчивости системы связи критически важных объектов и объектов критической информационной инфраструктуры // FISP-2021. Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации : сборник докладов III Всероссийской научной конференции (с приглашением зарубежных ученых), 29 ноября — 1 декабря, Ставрополь. 2021. С. 105-110.
5. Метод построения профиля функционирования сложной технической системы / О. С. Лаута [и др.] // Инженерный вестник Дона, 2023, № 2. [Электронный ресурс]. URL: ivdon.ru/ru/magazine/archive/n1y2023/8183.
6. Одоевский С. М., Лебедев П. В. Методика оценки устойчивости функционирования системы технологического управления инфокоммуникационной сетью специального назначения с заданной топологической и функциональной структурой // Системы управления, связи и безопасности. 2021. № 1. С. 152-189. DOI: 10.24411/2410-9916-2021-10107.
7. Петренко С. А. Концепция поддержания работоспособности киберсистем в условиях информационно-технических воздействий // Труды ИСА РАН. М. 2009. Т. 41. С. 175-193.
8. Дурняк Б. В., Машков О. А., Усаченко Л. М., Сабат В. И. Методология обеспечения функциональной устойчивости иерархических организационных систем управления. Институт проблем моделирования в энергетике : сборник научных статей. НАН Украины. Вып. 48, 2008. С. 3-21.
9. Королев А. Н. Функциональная устойчивость навигационно-информационных систем // Известия вузов. СПб.: Приборостроение. 2018. Т. 61. № 7. С. 559-565. DOI: 10.17586/0021-3454-2018-61-7-559-565.
10. Тарасов А. А. Функциональная реконфигурация отказоустойчивых систем : монография. М.: Логос, 2012. 152 с.

УДК 004.71

К ВОПРОСУ ИСПОЛЬЗОВАНИЯ ПРОТОКОЛОВ ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Рубцова Марина Андреевна, Сазонов Виктор Викторович
Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: 8902279299@mail.ru, vmktor-sazonov@yandex.ru

Аннотация. Анализ достоинств и недостатков протоколов динамической маршрутизации выполненный в имитационной модели сети передачи данных построенной на объектах комплексного оснащения показывает, что необходим контроль вопросов адаптации маршрутов, приоритезации трафика и повышение вероятности перехвата трафика.

Ключевые слова: объект комплексного оснащения; межсетевой экран; маршрутизатор; протоколы динамической маршрутизации; адаптация маршрутов; вероятность перехвата трафика.

ON THE ISSUE OF USING DYNAMIC ROUTING PROTOCOLS IN SPECIAL PURPOSE DATA TRANSMISSION NETWORKS

Marina Rubtsova, Viktor Sazonov
Military Academy of Communications Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails: 8902279299@mail.ru, vmktor-sazonov@yandex.ru

Abstract. The analysis of the advantages and disadvantages of dynamic routing protocols performed in a simulation model of a data transmission network built on complex equipment facilities shows that it is necessary to control the issues of route adaptation, traffic prioritization and increase the probability of traffic interception.

Keywords: object of complex equipment; firewall; router; dynamic routing protocols; route adaptation; probability of traffic interception.

Известно [1-3], что сеть передачи данных специального назначения (СПД СН) может быть построена на объектах комплексного оснащения (ОКО), каждый из которых включает средство доступа к сети оператора связи, коммутатор локальной сети с абонентами открытого сегмента, криптомаршрутизатор с межсетевым экраном, коммутатор и абонентские средства локальной сети закрытого сегмента. Для эффективного функционирования СПД СН в ОКО используются протоколы динамической маршрутизации (RIP v.2, OSPF, EIGRP и др.) учитывающие специфические требования к защите данных. Каждый из протоколов динамической маршрутизации имеет свои достоинства и недостатки [4, 5].

Достоинства:

– В больших гетерогенных СПД СН облегчение труда системных администраторов;
– Адаптивность маршрутов передачи данных в зависимости от текущего состояния СПД СН;
– Хорошая масштабируемость СПД СН;

– Уменьшение среднего времени нахождения пакета и как следствие минимизация затрат на его доставку получателю в СПД СН с разнородным трафиком.

Недостатки:

– Необходима высокая квалификация системных администраторов СПД СН;

– Сложности в решении вопросов приоритезации трафика;

– Возрастание нагрузки на оборудование СПД СН;

– Сложность контроля маршрута в СПД СН подверженной динамическим изменениям (повышение вероятности появления «петель» внутри сети, появление маршрута через неконтролируемые зоны);

– Увеличение вероятности перехвата трафика.

В докладе рассматриваются достоинства и недостатки протоколов динамической маршрутизации СПД СН. При конфигурировании элементов СПД СН, построенной на базе ОКО необходим контроль вопросов адаптации маршрутов, приоритезации трафика и повышение вероятности перехвата трафика.

СПИСОК ЛИТЕРАТУРЫ

1. Иванов В. Г. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи : монография. СПб.: ПОЛИТЕХ-ПРЕСС, 2018. 214 с.
2. Носов А. О., Житков А. П., Сазонов В. В., Файзулин В. В. Модель стационарной сети передачи данных / Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)», Санкт-Петербург, 28-30 октября 2020 г. : материалы конференции. Ч. 1. СПб: СПОИСУ, 2020. С. 95.
3. Сазонов В. В., Носов А. О. Моделирование сети передачи данных специального назначения // Перспективные направления развития отечественных технологий. Материалы V межрегиональной научно-практической конференции. Севастопольский государственный университет; Санкт-Петербургский институт информатики и автоматизации РАН. Севастополь, 2019. С. 212-214.
4. Венков С. С., Геннеберг А. Е., Филиппов И. Е. Актуальность использования протоколов динамической маршрутизации — RIP, OSPF в сети предприятия / EUROPEAN RESEARCH. X Международная научно-практическая конференция : сб. статей победителей : в 3 ч. 2017. С. 115-117.
5. Гайдаров И. О., Ерёмин О. Ю. Обзор технологических решений протоколов внутренней динамической маршрутизации OSPF и EIGRP // Теоретические и прикладные аспекты современной науки. 2014. №3-1. С. 44-48.

УДК 004.652.4

МЕТОД ОБНАРУЖЕНИЯ АНОМАЛИЙ В SQL-ЗАПРОСАХ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

Рюмина Светлана Алексеевна, Саенко Игорь Борисович
Военная академия связи имени Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: svetlanarumina66@gmail.com, ibsaen@mail.ru

Аннотация. Предлагается метод обнаружения аномалий в SQL-запросах, основанный на использовании различных моделей машинного обучения. Рассматривается применение метода «мешок слов» для выявления групп признаков для дальнейшего обучения моделей. Производится сравнительный анализ работы моделей машинного обучения и выявление наиболее точных классификаторов для обнаружения SQL-атак.

Ключевые слова: аномалия, база данных, машинное обучение, классификатор, безопасность данных.

MACHINE LEARNING-BASED ANOMALIE DETECTION METHOD IN SQL QUERIES

Ryumina Svetlana, Saenko Igor
The Military Academy of Telecommunications named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails: svetlanarumina66@gmail.com, ibsaen@mail.ru

Abstract. A method for detecting anomalies in SQL queries based on the use of various machine learning models is proposed. The application of the «bag of words» method to identify groups of features for further training of models is considered. A comparative analysis of the operation of machine learning models and the identification of the most accurate classifiers for detecting SQL attacks is carried out.

Keywords: anomaly, data base, machine learning, classifier, data security.

IT-отрасль является одной из самых развивающихся отраслей современной экономики, и внедрение машинного обучения становится все более распространенным явлением в ее процессах. Машинное обучение — это метод анализа данных, позволяющий компьютерной системе автоматически извлекать знания из опыта и использовать их для принятия решений без явного программирования. В IT-отрасли машинное обучение может быть применено для решения широкого спектра задач, таких как оптимизация производства, автоматизация процессов, анализ больших данных и многое другое [1].

Одной из актуальных областей применения машинного обучения является определение аномалий при работе с базами данных. Особенностью выявления аномальных действий пользователей является то, что атаки на базы данных реализуются через изменение SQL-запросов [2]. Например, запрос может осуществлять передачу учетных данных пользователя через веб-форму для доступа к сайту. Обычно подобные веб-формы сконфигурированы таким образом, чтобы принимать только определенные типы данных, такие как имя пользователя и пароль. Введенная информация сверяется с базой данных. Если все совпадает, пользователь сможет войти на сайт. А если нет — в доступе будет отказано. Однако, большинство веб-форм не имеют

механизмов, которые бы исключали ввод дополнительной информации в поле. Это дает злоумышленникам возможность передать в базу данных собственные запросы через поля ввода формы.

В данном докладе будет представлен метод обнаружения подобного рода SQL-запросов с помощью системы анализа данных и машинного обучения.

Основная часть. Предлагается метод обнаружения аномалий в SQL-запросах, основанный на использовании бинарных моделей классификации, таких как: NB (наивный Байес), RF (случайный лес), DT (дерево решений), GB (повышение градиента) [3].

Данный метод предполагает следующие этапы:

– формирование наборов данных для обучения моделей;
– выделение основных признаков для моделей машинного обучения;
– обучение моделей;
– выявление аномалий в запросах с использованием обученных моделей.

Наборы данных были взяты из регистрационных журналов СУБД. Каждую строку такого журнала можно представить совокупностью трех полей: время запроса; пользователь, являющийся автором запроса; полный текст SQL-запроса. Нормальный набор данных был сформирован из записей регистрационных журналов реально работающей базы данных контура управления учебным процессом АСУ высшего учебного заведения. База данных была создана в среде СУБД PostgreSQL. Записи регистрационных журналов соответствовали 10 минутам работы пользователей. Объем наборов данных варьировался от 20 до 30 тысяч записей.

Процесс обучения происходил на основе обработки данных и их классификации с помощью выбранных моделей машинного обучения. Выделение признаков для моделей машинного обучения производилось с помощью метода bag-of-word («мешок слов») [4]. Данный метод, при котором подсчитывается количество вхождений различных слов в текст запроса, позволяет в достаточной степени формализовать представление текста запросов.

Предложенный метод обнаружения аномальных SQL-запросов был реализован следующим образом. Формирование набора данных было реализовано в системе Orange 3.35 с помощью встроенных виджетов, работа которых основана на языке Python. Обучение и дальнейшее тестирование моделей также было реализовано в системе Orange 3.35. Объем данных, используемый для обучения, составлял 2000 записей. Дополнительно вручную были внесены аномальные SQL-запросы, составляющие 1 % от общего объема данных. Выявление аномалий в запросах с использованием обученных моделей проводилось после тестирования моделей. Для тестирования отводилось 20% исходного набора данных, в которые так же вносились аномальные запросы.

В ходе экспериментальной оценки предложенного метода были выявлены наиболее достоверные и эффективные модели машинного обучения с эффективностью (F-мерой), превышающей 0,96. Такими моделями оказались NB и GB.

В статье рассмотрен метод машинного обучения для обнаружения аномалий в SQL-запросах, основанный на использовании различных моделей машинного обучения. Метод включает четыре этапа, на которых производится формирование наборов данных для обучения моделей, выделение основных признаков для моделей машинного обучения, обучение моделей и выявление аномалий в запросах с использованием обученных моделей. Экспериментальная оценка предложенного метода подтвердила его высокую эффективность.

СПИСОК ЛИТЕРАТУРЫ

1. Саенко И. Б., Захарченко Р. И., Ясинский С. А., Грязев А. Н. Модели функционирования критической информационной инфраструктуры в условиях кибернетического противоборства // Информация и космос. 2018. № 2. С. 46-51.
2. Беляев А. В., Григоров А. С. Обнаружение атак на базы данных на основе оценки внутренней структуры результатов выполнения SQL-запросов // Научно-технический вестник Поволжья. 2012. № 2. С. 99-104.
3. Браницкий А. А., Саенко И. Б. Методика многоаспектной оценки и категоризации вредоносных информационных объектов в сети Интернет // Труды учебных заведений связи. 2019. Т. 5, № 3. С. 58-65.
4. Qader W. A., Ameen M. M., Ahmed B. I. An Overview of Bag of Words. Importance, Implementation, Applications, and Challenges // International Engineering Conference (IEC). 2019. Pp. 200-204.

УДК 004.0056

БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ И БЕЗОПАСНОСТЬ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Рязанцева Полина Сергеевна, Михайличенко Николай Валерьевич, Грибков Владимир Александрович, Ащеулов Сергей Викторович
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: 23esn2008@rambler.ru

Аннотация. Рассматриваются способы построения беспилотных летательных аппаратов, анализ вариантов использования БПЛА, инструменты использование дронов для обнаружения и контроля воздушного пространства над ЦОД, которые в свою очередь могут быть эффективным инструментом улучшения безопасности и реагирования на потенциальные угрозы.

Ключевые слова: БПЛА; безопасность; дрон; методы защиты; центр обработки данных.

UNMANNED AERIAL VEHICLES AND SECURITY DATA CENTERS

Ryazanceva Polina, Mihaylichenko Nikolay, Gribkov Vladimir, Asheulov Sergey
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: 23esn2008@rambler.ru

Abstract. Methods of building unmanned aerial vehicles, analysis of UAV use cases, tools for using drones to detect and control the airspace over the data center, which in turn can be an effective tool for improving security and responding to potential threats, are considered.

Keywords: UAV; security; drone; protection methods; data processing center.

Возрастающий объем дронов приводит к ряду проблем в области безопасности. Во-первых, существует риск аварий и столкновений с самолетами, другими дронами или людьми на земле. Несоблюдение правил полетов и незаконное использование дронов могут привести к серьезным последствиям. Во-вторых, существует угроза конфиденциальности и нарушения частной жизни. Дроны могут использоваться для незаконного съема фото и видео или для шпионажа. Это вызывает обеспокоенность как у частных лиц, так и у организаций.

Также существует опасность использования дронов для доставки запрещенных или опасных предметов, таких как наркотики или оружие. Это требует усиления мер контроля и регулирования использования дронов.

Для решения этих проблем необходимы строгие правила и законодательство, регулирующие использование дронов. Власти должны установить ограничения на высоту полета и места, где дроны могут использоваться. Также необходимо установить требования к лицам, имеющим право управлять дронами, а также меры по обеспечению безопасности полетов.

Компании, производящие дроны, также могут принять меры по повышению безопасности своих продуктов, например, включить дополнительные системы управления и автоматического избегания столкновений.

В целом, развитие отрасли дронов представляет много перспектив, но с ним также приходят сложности и риски в области безопасности. Регулирование и контроль становятся необходимыми, чтобы обеспечить безопасное и эффективное использование дронов.

Это событие подчеркнуло необходимость разработки более эффективных методов обнаружения и нейтрализации нежелательного использования дронов. Возможные решения включают в себя разработку технологий, способных автоматически определить и перехватить воздушные аппараты, осуществлять их навигацию и предотвращать возможные сбои.

Были предложены различные подходы к решению этой проблемы, включая использование радаров, обнаруживающих радиосигналы, отправляемые дронами, и систем, испускающих радарными сигналами, препятствующие нормальной работе дронов. Также были предложены методы, основанные на использовании технологий искусственного интеллекта для анализа и классификации данных, полученных от дронов, чтобы отличать нежелательные использования от легитимных.

Однако, разработка эффективных технологий обнаружения и нейтрализации дронов является сложной задачей. Необходимо учитывать различные типы дронов, их возможности и способы управления, а также возможные методы обхода систем защиты. Кроме того, безопасность и неприкосновенность легального использования дронов также должны быть обеспечены.

Для борьбы с угрозой, связанной с использованием дронов злоумышленниками, необходимо сотрудничество между правительственными органами, полицией, службами безопасности и промышленностью. Более тесная координация и обмен информацией между этими сторонами помогут эффективно противостоять таким инцидентам и минимизировать их последствия.

Это создает потенциальную угрозу для безопасности, так как дроны могут быть использованы для незаконного сбора информации, нарушения конфиденциальности и даже террористических актов. Без возможности обнаружения и отслеживания этих устройств, группа безопасности и быстрого реагирования на инциденты не может эффективно защитить зону безопасности.

Критическая важность решения этой проблемы вытекает из потенциальных последствий, которые могут возникнуть в результате неконтролируемого использования дронов. Непроизвольное или злонамеренное вторжение воздушных устройств в зону безопасности может вызвать серьезные последствия, включая потерю жизней, нарушение работоспособности систем и утечку конфиденциальной информации.

Поэтому необходимо приложить все усилия для разработки эффективных решений и обеспечения безопасности воздушного пространства. Группа безопасности и быстрого реагирования на инциденты должна быть особенно чувствительна к этой проблеме и принимать все необходимые меры для защиты зоны безопасности от угроз, связанных с дрона.

Поскольку роль дата-центров в обеспечении функционирования современной инфраструктуры, необходимой для функционирования и простым обывателям для поддержания привычного образа жизни, мониторинг инфраструктуры ЦОД и обеспечение высокого уровня безопасности становятся критически важными задачами [1].

Персонал ЦОД находится под растущим давлением, обусловленным необходимостью защиты инфраструктуры от угроз как физического, так и кибернетического характера. Любые сбои в работе дата-центра могут привести к катастрофическим последствиям.

Длительный период простоя ЦОД неизбежно влечет за собой значительные финансовые и репутационные потери, вызывая массовые сбои в работе предприятий, которые в настоящее время сильно зависят от беспрепятственной передачи и обработки данных с использованием инфраструктуры дата-центров.

И хотя в последние годы дата-центры стали гораздо более безопасными, умение реагировать на новые угрозы — это ключ к тому, чтобы быть на шаг впереди злоумышленников. Современные системы безопасности ЦОД обеспечивают значительный прогресс с точки зрения возможностей защиты периметра на земле, включая камеры видеонаблюдения, тепловизионные камеры и радары для отслеживания перемещений злоумышленников.

Размещаемые внутри ЦОД камеры и датчики используются для обнаружения и пресечения преступной деятельности. Но теперь операторам и владельцам корпоративных и коммерческих серверных ферм приходится считаться с новой угрозой, исходящей с небес [2, 3].

Использование специального программного обеспечения в дополнение к системам поддержания физической безопасности теперь позволяет обнаруживать дроны на основе излучаемых ими радиочастотных сигналов. Этот подход может быть использован для определения марки и модели более чем 2 сотен дронов, включая коммерческие, любительские и самодельные беспилотники, а также для точного определения местонахождения пилота каждого конкретного устройства.

Подобный подход гораздо продуктивнее, чем решение полагаться исключительно на глаза и уши сотрудников службы безопасности. Рассматриваемая технология способна предоставить операторам центров обработки данных заблаговременное предупреждение о приближении дрона, позволяя приблизительно понять намерения пилота устройства.

Использование дронов для обнаружения и контроля воздушного пространства над центром обработки данных может дать ряд преимуществ. Во-первых, это позволит обнаруживать любые несанкционированные дроны, которые могут пытаться проникнуть в ЦОД, что усилит общую безопасность. Во-вторых, дроны могут использоваться для мониторинга и контроля окружающей территории, что поможет предотвратить любые попытки несанкционированного доступа или кражи данных.

Интеграция этих данных с существующими системами управления видео позволит операторам быстро обнаруживать любые потенциальные угрозы и принимать соответствующие меры для их устранения. Например, если на дроне обнаруживается вооружение или другие опасные предметы, операторы могут вызвать службы безопасности для немедленного реагирования.

Кроме того, дроны могут использоваться для поиска уязвимых мест внутри ЦОД, таких как неисправности систем охлаждения или проблемы с безопасностью. Это позволит операторам ЦОД быстро устранять проблемы и поддерживать непрерывную работу.

Однако, необходимо учитывать возможные риски и ограничения при использовании дронов. Например, возможны сбои в работе дронов или их потенциальное использование злоумышленниками для проникновения в ЦОД. Поэтому важно разработать соответствующие протоколы безопасности и обучить персонал ЦОД по правилам использования дронов.

В целом, использование дронов для обнаружения и контроля воздушного пространства над ЦОД может быть эффективным инструментом улучшения безопасности и реагирования на потенциальные угрозы. Однако, должны быть приняты соответствующие меры безопасности и интеграции с существующими системами управления, чтобы обеспечить оптимальную эффективность и защиту центра обработки данных.

СПИСОК ЛИТЕРАТУРЫ

1. Докучаев В. А., Кальфа А. А., Маклачкова В. В. Архитектура центров обработки данных / Под редакцией проф. В. А. Докучаева. М.: Горячая линия-Телком, 2021. 240 с.
2. Семенов А. Б. Структурированные кабельные системы для центров обработки данных. М.: ДМК Пресс, 2019. 234 с.
3. TIA/EIA-942. Telecommunications Infrastructure Standard for Data Center (Телекоммуникационная инфраструктура для Центров Обработки Данных) Стандарт ANSI. // Программируя Вселенную. Квантовый компьютер и будущее науки / Сет Ллойд, 2019.

УДК 621.396.4

АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ АВТОМАТИЗАЦИИ ДОКУМЕНТООБОРОТА С УЧЕТОМ АНАЛИЗА РИСКОВ ИХ ЗАЩИЩЕННОСТИ

Саяркин Виталий Андреевич, Паращук Игорь Борисович
Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: vitaliysayarkin@gmail.com, shchuk@rambler.ru

Аннотация. В докладе приведены результаты исследования некоторых важных аспектов обеспечения информационной безопасности систем автоматизации документооборота, работающих с использованием трактов региональных телекоммуникационных сетей, с точки зрения анализа рисков их защищенности. Рассмотрены, в частности, вопросы классификации и градации угроз защищенности процедур обмена электронными документами по каналам и трактам современных региональных телекоммуникационных сетей. Эти результаты призваны помочь повысить степень обоснованности принимаемых решений при разработке и

аппаратно-программной реализации эффективных средств и комплексов обеспечения информационной безопасности для систем автоматизированной обработки электронных документов.

Ключевые слова: риски, информационная безопасность, электронный документооборот, угрозы, региональная телекоммуникационная сеть, электронный документ.

ASPECTS OF ENSURING INFORMATION SECURITY OF DOCUMENT MANAGEMENT AUTOMATION SYSTEMS, TAKING INTO ACCOUNT THE RISK ANALYSIS OF THEIR SECURITY

Sayarkin Vitaly, Parashchuk Igor
Military Academy of Communications Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails: vitaliysayarkin@gmail.com, shchuk@rambler.ru

Abstract. The report presents the results of a study of some important aspects of ensuring information security of document management automation systems operating using the paths of regional telecommunications networks, from the point of view of risk analysis of their security. In particular, the issues of classification and gradation of threats to the security of electronic document exchange procedures through channels and paths of modern regional telecommunication networks are considered. These results are intended to help increase the degree of validity of decisions taken in the development and hardware and software implementation of effective means and complexes for ensuring information security for automated electronic document processing systems.

Keywords: information security, risks, threats, electronic document management, regional telecommunication network, electronic document, incident, information security event.

Комплексы и системы автоматизации документооборота, часто называемые также системами электронного документооборота, представляют собой совокупность территориально распределенных автоматизированных технических (аппаратно-программных и региональных телекоммуникационных) средств и подсистем для многопользовательского обмена электронными документами (ЭД). Они призваны сопровождать все или почти все процедуры управления функционированием организации (министерства, учреждения, департамента) с иерархической структурой, имея целью обеспечение качественного и безопасного (защищенного) выполнения этой организацией своих задач [1-3].

Системы электронного документооборота используют каналы и тракты региональных телекоммуникационных сетей (РТКС). При этом, являясь одним из базовых элементов типовой IT-инфраструктуры региона или региональной организации практически любого масштаба, классическая система автоматизации документооборота (САДО) обеспечивает не только и не столько обмен ЭД, но также предполагает и создание этих ЭД, управление доступом к ним пользователей, распространение этих ЭД по каналам и трактам РТКС между пользователями САДО, но главное — реализацию эффективного контроля над потоками ЭД в региональной организации с иерархической структурой, создавая, тем самым, предпосылки для обеспечения высокого качества предоставляемых информационных услуг.

С точки зрения контента, предоставляемого САДО своим пользователям по каналам и трактам РТКС, принято различать: ЭД в виде активных ЭД и архивов (различают протоколы и алгоритмы создания и управления актуальными и не актуальными ЭД, т.е., архивами); электронные материалы (данные), не попадающие под определение ЭД, протоколы (механизмы) реализации бизнес-процессов и обеспечения гарантии взаимосвязи между бизнес-процессами на основе потоков ЭД и протоколов (механизмов) коллективного сотрудничества — совместной, групповой работы над конкретными ЭД. Не секрет, что весь этот контент, все эти ЭД и иные данные, создаваемые, хранимые и распространяемые в САДО по каналам и трактам РТКС, уязвимы, подвержены рискам модификации и уничтожения, нуждаются в дополнительных процедурах, обеспечивающих их информационную безопасность. Причем, особого внимания заслуживает контент САДО, распространяемый по открытым, не контролируемым каналам и трактам современных РТКС [4].

В этой связи особую актуальность для понимания глубины проблемы приобретают процедуры анализа и общей классификации возможных рисков информационной безопасности ЭД и иных ресурсов, создаваемых, хранимых и распространяемых в рамках САДО по каналам и трактам современных РТКС [5].

При этом компонентами САДО, напрямую подверженными рискам информационной безопасности, являются не только и не столько данные (информация, ЭД) и их носители, но и процессы обработки этих данных в рамках систем такого класса, включая передачу ЭД по каналам и трактам современных региональных телекоммуникационных сетей. С учетом того факта, что риски (угрозы) могут быть традиционно сгруппированы по нарушаемым аспектам информационной безопасности САДО, эти риски, как и для различных иных региональных телекоммуникационных систем, могут быть разделены на риски информационной безопасности с точки зрения нарушения конфиденциальности, нарушения целостности и нарушения доступности данных (ЭД), создаваемых, обрабатываемых и хранимых в рамках систем такого класса, а также передаваемых по каналам и трактам современных РТКС [6].

При этом считается, что наиболее серьезное значение имеют риски информационной безопасности САДО, связанные: с «утечкой» данных по техническим каналам взаимодействия между элементами САДО, а также по каналам и трактам региональных телекоммуникационных сетей; с возможным несанкционированным доступом

к данным, обрабатываемым и хранимым в рамках систем такого класса, а также передаваемым по каналам и трактам современных РТКС [5].

С точки зрения анализа и общей классификации, под кризисными событиями информационной безопасности для САДО с точки зрения нарушения конфиденциальности, могут пониматься такие явные и неявные риски, как: риски нарушения конфиденциальности автоматизированного рабочего места (АРМ) САДО — угроза непосредственного физического доступа к АРМ, когда потенциальный нарушитель заранее обладает данными идентификации (например, логин и пароль) легитимного пользователя или системного администратора САДО; риски воровства или перехвата данных (ЭД); риск нарушения конфиденциальности сервера операционной системы, на которой работает САДО — угроза загрузки на сервер вредоносного программного обеспечения, включая программы-шпионы, облегчающие потенциальный взлом САДО; риски нарушения конфиденциальности сервера САДО — угроза получения несанкционированного доступа напрямую к САДО, в обход сервера операционной системы, т.е., минуя, обходя базовую систему информационной безопасности; риски нарушения конфиденциальности сервера базы данных САДО — угроза получения частичного или полного контроль над САДО и доступа к наиболее важным ЭД, хранимым в этой базе данных; риски для каналов взаимодействия между компонентами САДО — угроза перехвата пакетов между АРМ и базовыми серверами САДО; риски для каналов и трактов региональных телекоммуникационных сетей, действующих в интересах САДО — угроза преднамеренной подмены маршрутов доставки ЭД.

Под кризисными событиями информационной безопасности с точки зрения нарушения целостности, могут пониматься риски, ориентированные на основной объект САДО — электронный документ: риски нарушения целостности ЭД, циркулирующих в САДО (с точки зрения злоумышленной модификации заранее определенных системой вида и качества этих ЭД, хранящихся в базе данных САДО); риски нарушения целостности, т.е., вида и качества резервных копий ЭД.

Более того, среди рисков информационной безопасности для САДО часто рассматривают: риски целостности — уничтожение или искажение информации, которые могут быть как непреднамеренными, так и умышленными; риски конфиденциальности — любые нарушения конфиденциальности, при которых информация становится известной лицам, не имеющим к ней доступ (кража информации); риски доступности — комплекс потенциальных угроз, нарушающих возможность получить своевременный и беспрепятственный доступ к информации пользователям, имеющим к ней права доступа; риски работоспособности системы — угрозы, реализация которой приводит к сбою в работе системы; риски невозможности доказательства авторства — комплекс угроз, выражающихся в том, что если в документообороте не используется электронная подпись, то нельзя доказать, что именно данный пользователь создал данный документ [7].

Таким образом, проведен анализ и рассмотрены отличительные особенности угроз и грани возможного ущерба, вызванных основными рисками информационной безопасности для электронного документооборота на базе современных региональных телекоммуникационных сетей. Предполагается, что учет этих особенностей и классификационных признаков позволит повысить степень обоснованности принимаемых решений по разработке и реализации высококачественных подсистем информационной безопасности для систем автоматизированной обработки электронных документов, использующих каналы и тракты региональных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Тищенко А. А. Автоматизация документооборота : учеб. пособие / А. А. Тищенко, Ю. М. Казаков, М. В. Терехов [и др.]. М.: Флинта. 2018. 108 с.
2. Коржук В. М., Попов И. Ю., Воробьева А. А. Защищенный документооборот.ч. 1: учеб.-метод. пособие — СПб: ИТМО, 2021. 67 с.
3. Селезнев А. В., Паращук И. Б., Саяркин В. А. Современный электронный документооборот в автоматизированных системах диспетчерского управления движением поездов: вопросы защиты информации // Материалы V-й международной научно-практической конференции «Инновационная железная дорога. Новейшие и перспективные системы обеспечения движения поездов. Проблемы и решения» : сборник статей // Под общей редакцией Яшина М. Г. Санкт-Петербург, Петергоф: ВИ (ЖДВ и ВОСО), 2022. С. 405-413.
4. Технологии и средства построения инфокоммуникационных систем специального назначения: Часть II: учебник / В. С. Авраменко, О. В. Беззубов, С. В. Беляев [и др.] ; под общ. ред. И. Б. Саенко. СПб.: ВАС, 2021. 416 с.
5. Ложников П. С., Жумажанова С. С. Об угрозах безопасности сведений ограниченного доступа в системах смешанного документооборота и правовом регулировании в области применения цифровых подписей с биометрической активацией // Доклады Томского государственного университета систем управления и радиоэлектроники. 2018. Т. 21, № 4. С. 35-43.
6. Десницкий В. А., Паращук И. Б. Анализ и обеспечение защищенности данных пользователей беспроводных сенсорных сетей: показатели доступности, целостности и конфиденциальности // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7. СПОИСУ. СПб.: 2019. С. 34-38.
7. Ушаков Н. О., Сибикина И. В., Космачева И. М. Информационная безопасность систем электронного документооборота // Техническая эксплуатация водного транспорта: проблемы и пути развития // Материалы Третьей международной научно-технической конференции. 2021. С. 70-74.

УДК 004.0056

РАЗВИТИЕ КВАНТОВЫХ ТЕХНОЛОГИЙ И ИХ ВЛИЯНИЕ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Сергеев Валерий Юрьевич, Михайличенко Николай Валерьевич,
Грибков Владимир Александрович, Мишутин Никита Вячеславович
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: 23esn2008@rambler.ru

Аннотация. Рассматриваются перспективы развития и создания квантового компьютера, его сравнения с компьютером, работающем на транзисторах, способы защиты от атак злоумышленника с помощью квантовых компьютеров, а также анализ факторов влияющих на безопасность центров обработки данных.

Ключевые слова: квантовые технологии; информационная безопасность; исследования; интеграция; методы защиты; центр обработки данных.

THE DEVELOPMENT OF QUANTUM TECHNOLOGIES AND THEIR IMPACT ON THE INFORMATION SECURITY OF DATA CENTERS

Sergeev Valeriy, Mihaylichenko Nikolay, Gribkov Vladimir, Mishutin Nikita
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: 23esn2008@rambler.ru

Abstract. The prospects for the development and creation of a quantum computer, its comparison with a computer running on transistors, ways to protect against attacks by an attacker using quantum computers, as well as an analysis of factors affecting the security of data centers are considered.

Keywords: quantum technologies; information security; research; integration; protection methods.

Квантовые технологии представляют собой новую эру в развитии информационных технологий. Квантовый компьютер работает на основе квантовых битов (qubits), которые могут находиться в неопределенном состоянии, что позволяет выполнять операции намного быстрее, чем на традиционных компьютерах [1].

Одной из главных проблем при создании квантовых компьютеров является сохранение состояния кубитов, наименьших единиц информации в квантовом компьютере (аналог бита в обычном компьютере), использующаяся для квантовых вычислений. Для этого требуется высокая степень изоляции от внешних воздействий. В настоящее время существуют несколько подходов к созданию квантовых компьютеров, но большинство из них еще не достигли коммерческой зрелости.

Сравнение квантовых компьютеров с традиционными компьютерами показывает, что квантовые компьютеры могут быть намного быстрее в решении определенных задач, таких как факторизация больших чисел и решение определенных задач оптимизации. Однако для большинства задач, связанных с обработкой данных, традиционные компьютеры все еще являются более эффективными.

Квантовые технологии также могут быть использованы для обеспечения информационной безопасности в центрах обработки данных (ЦОД). Например, квантовая криптография позволяет создавать ключи шифрования, которые невозможно взломать с помощью традиционных методов. Кроме того, квантовые компьютеры могут использоваться для быстрого поиска определенных данных в больших базах данных системы хранения центров обработки данных [2, 5-7].

Однако квантовые компьютеры также могут быть использованы злоумышленниками для взлома систем безопасности ЦОД. Например, квантовый компьютер может легко расшифровать данные, зашифрованные с помощью традиционных методов шифрования. Для защиты от таких атак необходимы новые методы защиты, которые будут устойчивы к квантовым вычислениям.

Таким образом, развитие квантовых технологий представляет собой огромный потенциал для различных областей, включая информационную безопасность. Однако для полного использования этого потенциала необходимо решить ряд технических и научных проблем.

Квантовые технологии представляют собой новый уровень развития информационных технологий, который может привести к изменению существующей системы защиты информации. Квантовые компьютеры могут обрабатывать огромные объемы данных за считанные секунды, что может значительно повысить эффективность криптографических алгоритмов. Однако, это также может привести к нарушению безопасности информации в ЦОД, поскольку существующие методы шифрования, которые используются в настоящее время, могут быть легко взломаны квантовыми компьютерами [3, 4].

В связи с этим, разработчики информационной безопасности начали искать новые методы защиты информации, которые могут обеспечить ее безопасность в условиях развития квантовых технологий. Одним из таких методов является квантовая криптография, которая использует фундаментальные законы квантовой механики для защиты информации.

Квантовая криптография основывается на использовании свойств квантовых систем, таких как суперпозиция и взаимозависимость состояний, для создания криптографических ключей. Эти ключи обеспечивают абсолютную безопасность передачи информации, поскольку любое попытка перехвата информации будет приводить к изменению ее состояния и, следовательно, к обнаружению нарушения.

Однако, квантовая криптография все еще находится в стадии разработки и тестирования, и ее практическое применение может быть ограничено высокой стоимостью и сложностью реализации. Тем не менее, это один из важных направлений в развитии информационной безопасности в условиях цифровой экономики.

Кроме квантовой криптографии, существуют и другие методы защиты информации от квантовых атак. Например, можно использовать алгоритмы, которые не зависят от факторизации больших чисел или дискретного логарифма, которые могут быть решены квантовыми компьютерами. Также можно использовать методы, которые обнаруживают попытки перехвата информации, например, через изменение состояния квантовых битов.

В целом, развитие квантовых технологий представляет как потенциальную угрозу для информационной безопасности, так и возможность для создания новых методов защиты информации. Разработчики информационной безопасности должны быть готовы к изменениям в технологической среде и постоянно совершенствовать свои методы защиты, чтобы обеспечить безопасность передачи и хранения информации в условиях быстрого развития квантовых технологий.

Способы квантовых кибератак могут включать в себя использование квантовых компьютеров для ломки криптографических ключей, перехвата и изменения информации, а также атак на квантовые сети и устройства. Кроме того, возможны и другие способы использования квантовых технологий для целей кибератак, которые могут быть еще неизвестны или недостаточно изучены.

Некоторые другие возможные способы квантовых кибератак могут включать использование квантовых алгоритмов для решения сложных математических задач, таких как поиск распределения наибольшего потока в графе или оптимизация функций. Кроме того, квантовые системы могут использоваться для создания спама, фишинга и других видов социальной инженерии.

Квантовые кибератаки могут также включать в себя использование квантовых алгоритмов для взлома защиты информационных систем, а также использование квантовых технологий для создания и распространения вредоносных программ и компьютерных сетей, состоящих из некоторого количества хостов с запущенными ботами — автономным программным обеспечением. Кроме того, квантовые кибератаки могут использовать квантовую телепортацию для передачи информации без возможности ее перехвата.

Также возможно использование квантовых защищенных каналов связи для передачи конфиденциальной информации между злоумышленниками. Квантовые кибератаки могут быть очень опасными, поскольку квантовые вычисления могут взломать защиту, которая кажется неприступной для классических вычислений. Поэтому разработчики систем информационной безопасности должны учитывать возможные квантовые угрозы и принимать меры для защиты от них.

Еще одним возможным способом квантовой кибератаки является использование квантовых запутанных состояний для передачи секретных сообщений между злоумышленниками. Это возможно благодаря особенностям квантовой механики, которые позволяют передавать информацию таким образом, что любая попытка перехвата сообщения приведет к его изменению или уничтожению.

В целом, квантовые кибератаки могут иметь множество различных форм и методов, включая комбинацию нескольких технологий и подходов. Чтобы защититься от них, необходимо обеспечивать безопасность своих сетей и устройств, использовать надежные алгоритмы шифрования и мониторинг информационной безопасности.

Таким образом, разработка и создание квантового компьютера является перспективным направлением в развитии информационных технологий. Однако, необходимо учитывать возможность использования квантовых компьютеров злоумышленниками для проведения кибератак, что требует разработки методов защиты и обеспечения безопасности информации. При этом, не следует забывать о существующих компьютерах, работающих на транзисторах, которые продолжают оставаться актуальными и необходимыми во многих сферах деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Химено-Сеговиа М., Хэрриган Н., Джонстон Э. Программирование квантовых компьютеров. Базовые алгоритмы и примеры кода. СПб : Питер, 2021. 340 с.
2. Силва В. Разработка с использованием квантовых компьютеров. СПб : Питер, 2020. 352 с.
3. TIA/EIA-942. Telecommunications Infrastructure Standard for Data Center (Телекоммуникационная инфраструктура для Центров Обработки Данных) Стандарт ANSI // Программируя Вселенную. Квантовый компьютер и будущее науки / Сет Ллойд, 2019.
4. Лисецкий Ю. М. Построение современного территориально-распределенного центра обработки данных // Программные продукты и системы. № 2, 2008.
5. Паращук И. Б., Михайличенко Н. В. Эффективность современных центров обработки данных. // Материалы III-й Межрегиональной НПК Перспективные направления развития отечественных информационных технологий. Севастополь : СевГУ, 2017. С. 24-26.
6. Докучаев В. А., Кальфа А. А., Маклачкова В. В. Архитектура центров обработки данных / под редакцией проф. В. А. Докучаева. М. : Горячая линия-Телком, 2021. 240 с.
7. Семенов А. Б. Структурированные кабельные системы для центров обработки данных. М.: ДМК Пресс, 2019. 234 с.

УДК 621.391 (075.8)

ПРИМЕНЕНИЕ СРЕДСТВ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ В БАЗАХ ДАННЫХ

Скоропад Александр Витальевич[1], Ильина Ольга Борисовна[2], Купчиненко Ольга Павловна[2]

[1]Санкт-Петербургский филиал — «ЛОНИИР» (ФГБУ НИИР),
Большой Смоленский пр., 4, Санкт-Петербург, 192029, Россия

[2]Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Аннотация. Проведен анализ метода резервного копирования и восстановления информации SQL-дамп в защищенной СУБД PostgreSQL из состава операционной системы специального назначения Astra Linux SE. Проанализированы преимущества и недостатки программных средств резервного копирования и восстановления

информации в СУБД. Для упрощения решения задачи резервного копирования и восстановления информации рассмотрено программное средство PgAdmin 3.

Ключевые слова: операционная система специального назначения; система управления базами данных; база данных; защита информации; резервное копирование и восстановление информации; дамп.

USE OF THE TOOLS FOR BACKUP AND RECOVERY OF INFORMATION IN DATABASES

Skoropad Aleksandr[1], Ilina Olga[2], Kupchinenko Olga[2]

[1]The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

[2]The M.I. Krivosheev Radio Research & Development Institute. LENINGRAD BRANCH — «LONIIR»
4 Bolshoy Smolensky Av, St. Petersburg, 192029, Russia

e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Abstract. The analysis of the method of backup and recovery of information SQL-dump in a protected DBMS PostgreSQL from the operating system of a special purpose Astra Linux SE is carried out. The advantages and disadvantages of software tools for backup and recovery of information in DBMS are considered. To simplify the task of backing up and restoring information, the PgAdmin 3 software tool is considered.

Keyword: operating system of a special purpose; database management system; database; information security; backup and recovery of information; dump.

В современном мире практически ни одна автоматизированная система управления не обходится без баз данных (БД). Защита информации в БД, в отличие от защиты данных в файлах, имеет ряд особенностей:

необходимость учета функционирования системы управления БД (СУБД) при выборе механизмов защиты;

разграничение доступа к информации реализуется не на уровне файлов, а на уровне БД.

Применение СУБД для создания БД в интересах должностных лиц позволяет решать задачи быстрого поиска информации, необходимой для работы должностных лиц, реализовать многоуровневую защиту информации, обеспечить разграничение доступа пользователей к ресурсам БД и управление информационными потоками [1].

Современная защищенная СУБД PostgreSQL 9.6 в операционной системе специального назначения (ОС СН) «Astra Linux Special Edition», релиз Смоленск, с встроенными средствами защиты информации предназначена для разработки информационных систем и систем управления для работы с конфиденциальной информацией и с информацией, содержащей сведения, составляющие государственную тайну [2].

Для защиты информации в БД, для надежного и быстрого восстановления работы БД в состав СУБД PostgreSQL 9.6 входят средства резервного копирования и восстановления информации (РКВИ) [3].

Один из методов РКВИ в СУБД PostgreSQL 9.6 — выгрузка в SQL.

Метод основан на генерации текстового файла, который содержит команды SQL (SQL-дамп). Дамп БД — это файл, содержащий инструкции языка SQL, которые создают точную копию структуры и содержимого БД. Эти команды SQL при выполнении на сервере создают новую БД, копию той, что была на момент выгрузки (исходное состояние БД). Для создания новой БД в PostgreSQL применяется программное средство pg_dump [3].

Программа pg_dump может создавать файлы в различных форматах, отличных от исходного формата файлов БД. Эта утилита предоставляет возможность параллельной обработки данных и удобное управление восстановлением данных.

Процедуру резервного копирования можно выполнять с любого удалённого компьютера, с которого есть доступ к БД.

Утилита pg_dump не использует для своей работы специальные привилегии. Для ее работы, в первую очередь, требуется задание дискреционных права доступа на чтение тех таблиц БД [4], которые необходимо копировать. Поэтому для копирования всей БД её необходимо запускать с правами суперпользователя СУБД.

Одним из главных преимуществ pg_dump по сравнению с другими средствами РКВИ является возможность загрузки утилиты в любые новые версии PostgreSQL, другие средства РКВИ строго зависят от версии сервера.

Метод с применением pg_dump так же будет работать при переносе БД на другую машинную архитектуру, например, при переносе с 32-битной на 64-битную версию сервера.

Дампы, создаваемые pg_dump, являются внутренне согласованными, то есть, дамп представляет собой снимок БД на момент начала запуска pg_dump. Утилита не блокирует другие операции с БД во время своей работы.

Программа pg_dump выгружает только одну БД в один момент времени и не включает в дамп информацию о ролях и табличных пространствах. Для удобства создания дампа всего содержимого кластера БД (набора БД, управляемого одним экземпляром запущенного сервера БД) предоставляется утилита pg_dumpall.

Утилита pg_dumpall предназначена для записи всех БД кластера PostgreSQL в один файл в формате скрипта. Этот файл содержит команды SQL. С помощью команды psql, можно восстановить все БД. Для формирования этого файла вызывается pg_dump для каждой БД в кластере.

Утилита pg_dumpall также выгружает глобальные объекты, общие для всех БД, то есть роли и табличные пространства. Программа pg_dump не сохраняет эти объекты.

pg_dumpall выдаёт команды, которые заново создают роли, табличные пространства и пустые БД, а затем вызывает для каждой базы pg_dump. Таким образом, хотя каждая БД будет внутренне согласованной, состояние разных БД не будет синхронным.

Процесс восстановления дампа.

Текстовые файлы, созданные pg_dump, предназначаются для последующего чтения программой psql. Общий вид команды для восстановления дампа:

psql имя_базы < файл_дампа

где файл_дампа — это файл, содержащий вывод команды pg_dump. БД, заданная параметром имя_базы, не будет создана данной командой, так что необходимо создать её из базы template0 перед запуском psql (например, с помощью команды createdb -T template0 имя_базы). Программа psql принимает параметры, указывающие на сервер, к которому осуществляется подключение, и имя пользователя.

Перед восстановлением SQL-дампа все пользователи, которые владели объектами или имели права на объекты в выгруженной БД, должны быть уже созданы. Если их нет, при восстановлении будут появляться ошибки пересоздания объектов с изначальными владельцами и/или правами.

Утилита pg_restore предназначена для восстановления БД PostgreSQL из архива, созданного командой pg_dump в любом из не текстовых форматов. Она выполняет команды, необходимые для восстановления того состояния БД, в котором база была сохранена. При наличии файлов архивов, pg_restore может восстанавливать данные избирательно или даже переупорядочить объекты перед восстановлением.

Утилита pg_restore работает в двух режимах:

– указывается имя БД, pg_restore подключается к этой БД и восстанавливает содержимое архива непосредственно в неё;

– имя БД не указывается, создаётся SQL-скрипт с командами, необходимыми для пересоздания БД.

Скрипт затем выводится в файл или в стандартное устройство вывода. Сформированный скрипт будет в точности соответствовать выводу pg_dump в простом текстовом формате. Поэтому некоторые из параметров, управляющих выводом, аналогичны параметрам pg_dump.

Решение задачи РКВИ можно выполнять с помощью программного средства PgAdmin 3.

PgAdmin 3 — графическая утилита, консоль комплексного проектирования и управления БД для БД PostgreSQL. Работа в PgAdmin 3 упрощает решение задачи по РКВИ в БД.

PgAdmin 3 для экспорта/импорта БД использует стандартные консольные утилиты, в частности pg_dump, pg_dumpall и pg_restore, которые по умолчанию входят в состав PostgreSQL 9.6.

Например, для копирования и восстановления БД в PgAdmin 3 необходимо создать копию БД, затем создать пустую БД и восстановить в пустую БД все данные, используя созданную ранее копию.

Таким образом, благодаря PgAdmin 3, не нужно писать и выполнять команды в командной строке, все это делает PgAdmin 3, настраивать все параметры можно в графическом интерфейсе.

РКВИ методом SQL-дамп рекомендуется для применения в случае работы с БД большого количества пользователей с различными правами доступа. SQL-дамп защитит информацию в БД и позволит восстановить ее работу в кратчайшие сроки.

СПИСОК ЛИТЕРАТУРЫ

1. Ильина О. Б., Купчиненко О. П., Скоропад А. В. Механизмы разграничения доступа к данным в СУБД в среде операционной системы специального назначения Astra Linux SE // Региональная информатика : материалы XVII Санкт-Петербургской международной конференции, СПб, 28-30 октября 2020 г. СПБ: СПОИСУ, 2020. Т. 1. С 79-81.
2. Ильина О. Б., Купчиненко О. П., Скоропад А. В. Разграничение доступа к данным в СУБД из состава операционной системы специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. СПб: СпбГУТ, 2021. С. 259-263.
3. Ильина О. Б., Купчиненко О. П., Скоропад А. В. Резервное копирование и восстановление информации в современных защищенных СУБД // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. СПб: СпбГУТ, 2022. Т. 2. С. 249-252.
4. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. СПб.: СПбГУТ, 2018. Т. 2. С 356-360.

УДК 621.396

ПОСТРОЕНИЕ СИСТЕМЫ КОМПЬЮТЕРНОЙ ПОДДЕРЖКИ ПРОВЕДЕНИЯ СПЕЦИАЛЬНЫХ УЧЕНИЙ (ИГР)

Солодухин Борис Владимирович, Пантюхин Олег Игоревич, Ковалёв Игорь Станиславович, Пащенко Василий Владимирович, Рябов Геннадий Анатольевич

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mail: boris.soloduxin@yandex.ru, p_oleg99@mail.ru, iskova@yandex.ru, vvpash@mail.ru, grif999@mail.ru

Аннотация. Доклад посвящен анализу проблемы и основным направлениям построения системы компьютерной поддержки проведения специальных учений (игр). В основу архитектуры системы компьютерной поддержки проведения учений положена логико-эвристическая модель процесса обучения на основе схемы ориентировочных действий и материализации действий обучающихся. Суть модели заключается в базировании

сценария на логической структуре изучаемого предмета и изучении каждого элемента логической структуры на основе ориентировочной и материализованной деятельности обучаемого, формализуемой при помощи специального набора базовых фрагментов — модулей сценария.

Ключевые слова: учения, система компьютерной поддержки, информационная система, логическая структура.

BUILDING A COMPUTER SUPPORT SYSTEM SPECIAL EXERCISES (GAMES)

Solodukhin Boris, Pantyukhin Oleg, Kovalev Igor, Pashchenko Vasily, Ryabov Gennady
Military Academy of Communications Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mail: boris.soloduxin@yandex.ru, p_oleg99@mail.ru, iskova@yandex.ru, vvpash@mail.ru, grif999@mail.ru

Abstract. The report is devoted to the analysis of the problem and the main directions of building a computer support system for conducting special exercises (games). The architecture of the computer support system for conducting exercises is based on a logical-heuristic model of the learning process based on a scheme of orienting actions and materialization of students' actions. The essence of the model is to base the scenario on the logical structure of the subject being studied and study each element of the logical structure on the basis of the student's orienting and materialized activity, formalized using a special set of basic fragments — scenario modules.

Keywords: exercises, computer support system, information system, logical structure.

При создании системы компьютерной поддержки проведения учений (СКППУ) учитывается ряд принципов:

- принцип объектно-ориентированного моделирования при построении картины предметной области;
- принцип динамической структуры;
- принцип полноты информационного пространства;
- принцип интеграции информационного пространства;
- принцип децентрализации информационного хранилища;
- принцип компонентной сборки прикладных режимов.

Поскольку принципы противоречивы, нужно искать компромисс между каждым из них. Данное обстоятельство обуславливает необходимость разработки структуры системы поддержки проведения учений, способной обеспечить достижение требуемых значений показателей эффективности проведения учений. Архитектурное построение современных информационных систем, используемых в качестве автоматизированных обучающих систем, отличается широким спектром программных и технических средств. Большое влияние на принимаемые решения оказывают такие факторы, как тип ЭВМ, объем и структура базы данных, расположение рабочих станций, средств передачи данных и т.п. Однако для значительного числа приложений могут употребляться стандартные решения по архитектурному построению информационных систем (ИС), которые апробированы и хорошо зарекомендовали себя на практике [1]. Информационные системы на основе локальной вычислительной сети (ЛВС) и применяемых электронных ресурсов для СКППУ высшего военного учебного заведения являются более предпочтительными по сравнению с централизованными ИС [2]. Информационные системы с централизованной обработкой данных используют программно-технические средства, обладающие жестким составом и конфигурацией. Однако в процессе эксплуатации ИС часто изменяются требования как к ее функциональным характеристикам, так и к архитектуре построения, что приводит к необходимости эволюции используемых программно-технических средств. Средства гибкого объединения в единую коммуникационную среду разнотипного вычислительного оборудования информационной системы были предложены и отработаны в рамках локальных вычислительных сетей, которые получили широкое распространение. Распределенная обработка информации, обеспечиваемая локальными вычислительными сетями, становится одной из основных альтернатив централизованной обработке. Естественно, что появление ЛВС привело к созданию на их основе новых архитектурных конфигураций, используемых для построения диалоговых информационных систем и хранилищ информации [2]. В таких архитектурах предусмотрено открытое подключение и использование вычислительных ресурсов с помощью единой передающей среды без пересмотра принципов взаимодействия ранее установленного вычислительного оборудования.

Анализ [1, 3] показал, что в основу архитектуры системы компьютерной поддержки проведения специальных учений (игр) целесообразно положить логико-эвристическую модель процесса обучения на основе схемы ориентировочных действий и материализации действий обучающихся. Суть модели заключается в базировании сценария на логической структуре (ЛС) изучаемого предмета и изучении каждого элемента ЛС на основе ориентировочной и материализованной деятельности обучаемого, формализуемой при помощи специального набора базовых фрагментов — модулей сценария учений.

Логическая структура предмета, разрабатываемая как иерархическая, упорядоченная система понятий, явлений, утверждений и методов изучаемого предмета, должна отражать реально существующие связи названных предметов. С каждым элементом структуры связываются определенные параметры, характеризующие его как учебный элемент логической структуры. Такими параметрами являются: цель; мотивация изучения; классы решаемых задач; условия, управляющие развитием сценария.

Цель обучения выражается в терминах текущих характеристик обучаемого. Пока цель не достигнута, повторяется следующая последовательность действий:

– генерируется очередная задача на основании текущего состояния обучаемого и методики обучения (задача понимается широко как любая информация, требующая ответных действий обучаемого);

– ответ обучаемого сравнивается с эталонным решением и на основании различий производится диагностика ошибок обучаемого;

– по результатам диагностики корректируются текущие характеристики обучаемого.

В соответствии с данной моделью процесса обучения СКППУ можно рассматривать как совокупность следующих компонентов: интеллектуальный интерфейс; система управления обучением; система проверки решений; модель слушателя; система решения задач в данной предметной области (ПрО). Все участники учений представлены как слушатели (обучаемые) и руководитель (руководители) — обучающие.

Система по решению задач предназначена для выработки эталонного решения задачи. Она представляет собой программы поиска или выбора решения данной задачи на конечного (возможно большого) набора решений если обучение ведется на заранее заготовленной совокупности задач.

Система проверки решений предназначена для выявления неправильных представлений обучаемого об изучаемой ПрО на основе сравнения его ответа с эталонным. Цель ее — диагностика. Симптомы выводятся на основании различия в ответах обучаемого и системы по решению задач, а результатами являются изменения текущих характеристик обучаемого (модели слушателя).

Система управления обучением представляет собой систему по планированию в ограничениях, накладываемых имеющимся учебным материалом. Система управления обучением также формализует знания эксперта-методиста о методиках обучения.

Интеллектуальный интерфейс служит для диалогового взаимодействия пользователей с системой. Эстетика и эргономика интерфейса определяют эффективность работы пользователей в большей степени, чем его функциональные возможности. Поэтому интерфейс должен обеспечивать работу на новом уровне, не подавляющем индивидуальности пользователей, понятном и открытом для настройки и модификации.

Исследования показали, что для реализации целесообразно выбирать смешанную структуру диалога, включающую следующие типы диалога: вопрос-ответ; меню; на основе экранных форм; на базе команд.

Этот выбор подтверждает следующие преимущества меню ориентированного интерфейса:

– высокая стандартизация функций выборки;
– простота программной реализации;
– упрощенная логика обработки программ;
– доступность в работе пользователей без предварительной подготовки;
– ориентация на конечного пользователя;
– адаптивность;
– восстанавливаемость при ошибках.

Следующим элементом является *модель слушателя*. Под *моделью слушателя* понимается анализ знаний руководителя учений (самой обучающей системы) о слушателе, используемые для организации процесса обучения. Модель слушателя включает знания об:

– общих характеристиках слушателя, не зависящих от предметной области (например, психофизиологические данные, такие как возраст, скорость реакции, способность к абстрактному мышлению и т. п.);

– отношении слушателя к учебному материалу, т.е. насколько полно и глубоко он владеет знаниями и умениями по изучаемому предмету;

– истории взаимодействия самой системы компьютерной поддержки проведения учений и слушателя.

Предварительные знания слушателя и цель обучения формулируются как требования к начальному и заключительному состоянию модели слушателя.

В настоящее время разработано несколько моделей обучаемого [3]. Для реализации СКППУ выбрана модель фиксирующего типа — векторная модель, которая каждому изучаемому понятию и умению ставить в соответствие элемент, принимающий значения «знает-не-знает» или «умеет-не-умеет». Состояние знаний слушателя определяется набором значений элементов вектора, а число возможных состояний равно 2^n, где n — размерность вектора, т.е. суммарное количество изучаемых понятий и умений.

Результаты выполнения заданий слушателей, выраженные в той или иной форме, представляются как неизвестный образ X. Факт наличия ошибки при выполнении задания имеет место, если расстояние между образом ответа и эталоном будет больше установленного порогового уровня (M). Чем больше расстояние между образами ответа обучаемого и эталоном, тем больше величина ошибки и тем меньше степень усвоения учебного материала.

Взаимодействие системы компьютерной поддержки проведения учений с обучаемым происходит следующим образом.

Система по управлению учением формирует в соответствии с текущей целью очередное задание для слушателя, которое передается одновременно и системе по решению задач.

Далее система проверки решений сравнивает решение обучаемого с решением, полученным системой по решению задач, и на основании различий пытается установить, какие неправильные представления обучаемого о ПрО могли привести к расхождениям.

В результате диагностики меняется представление СКППУ об обучаемом, отраженное в модели слушателя, и управление передается системе управления обучением, которая уточняет текущую цель и формирует новое задание. Взаимодействие со слушателем происходит через интеллектуальный интерфейс.

СПИСОК ЛИТЕРАТУРЫ

1. Прокопенко Н. Ю. Системы поддержки принятия решений на базе Deductor Studio Academic 5.3: учеб. пособие. Нижегородский государственный архитектурно-строительный университет. Н. Новгород: ННГАСУ, 2017. 188 с.
2. Юдин А. А., Пантюхин О. И., Чирушкин К. А. Применение электронных ресурсов в образовательном процессе высшего военного учебного заведения / Психолого-педагогические проблемы военного образования : сб. научно-педагогических трудов. Вып. 7 / под науч. ред. И. И. Соколовой, В. А. Митраховича, А. Р. Моисеева. СПб.: ВАС, 2017. 611 с. С. 427-434.
3. Будашевский В. Г. Логико-эвристический метод решения проблем, анализ возможности верификации или фальсификации интуитивных решений. Миасс: Филиал ФГБОУ ВПО Южно-Уральский государственный университет (НИУ), 2016. С. 61-75.

УДК 621.391

ПРЕДИКТИВНЫЙ КОНТРОЛЬ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ СЛОЖНОЙ ТЕХНИЧЕСКОЙ СИСТЕМЫ

Тесля Сергей Петрович, Остроумов Олег Александрович, Шинкарев Семен Александрович
Военная академия связи имени Маршала Советского Союза С.М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: oleg-26stav@mail.ru, tsp123@yandex.ru, se_men82@mail.ru

Аннотация. В докладе рассмотрен поход к обеспечению функциональной устойчивости системы, основанный на предиктивном ее контроле, позволяющем выявлять и прогнозировать изменения состояния системы. Предложены требования, которые должны предъявляться к современному предиктивному контролю, исходя из потребностей системы управления.

Ключевые слова: критичность, предиктивный контроль, сложная техническая система, функциональная устойчивость.

PREDICTIVE CONTROL OF THE FUNCTIONAL STABILITY OF A COMPLEX TECHNICAL SYSTEM

Sergey Teslya, Oleg Ostroumov, Semyon Shinkarev
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: oleg-26stav@mail.ru, tsp123@yandex.ru, se_men82@mail.ru

Abstract. The report considers an approach to ensuring the functional stability of the system, based on its predictive control, which makes it possible to identify and predict changes in the state of the system. The requirements that should be made to modern predictive control, based on the needs of the control system, are proposed.

Keywords: criticality, predictive control, complex technical system, functional stability.

Зависимость систем, объектов от других систем, объектов, своих элементов определяет необходимость обеспечения их устойчивого функционирования. В современном мире такая зависимость часто становится критичной, т.е. возникает ситуация, когда результат функционирования одной системы зависит от другой системы, объекта, какого-либо элемента системы. Нарушению устойчивого функционирования систем способствует преднамеренное или непреднамеренное воздействие различных дестабилизирующих факторов, количество которых с каждым годом растет [1, 2].

Последствия воздействия таких факторов, даже в условиях работоспособного состояния системы, могут быть разными и проявить себя могут не сразу, а через определенное время. Для выявления последствий воздействия на систему и ее элементы различных дестабилизирующих факторов необходимо осуществлять контроль ее функционирования, при этом, для систем реального времени [3, 4] контроль должен быть предиктивным и позволять не только выявлять последствия воздействия, но и прогнозировать последствия нарушения того или иного процесса в системе.

Контроль функционирования является одним из элементов цикла управления, который позволяет реализовать обратную связь по реагированию системы, ее подсистемы управления на события в системе. Результаты контроля в той или иной мере позволяют определить состояние системы и ее элементов в любой момент времени.

При рассмотрении предиктивного контроля возникает задача обеспечения полноты, своевременности и достоверности контроля. Для решения данной задачи необходимо формирование адекватного задания на контроль. В качестве такого средства предлагается использовать профиль функционирования системы, который представляет собой совокупность характеристик, правил функционирования системы [5, 6].

Построение автоматизированной системы предиктивного контроля процесса функционирования СТС, реализующая весь перечень ее потребностей, позволяющих, в первую очередь, обеспечить ее устойчивое функционирование обусловлено потребностями современных СТС, систем управления, получать информацию в режиме реального времени. Результаты анализа систем контроля функционирования сложных технических

систем показали возрастающую роль информационно технических систем (ИТС), выступающих в качестве интеграторов различных систем контроля и мониторинга и представляющих собой совокупности баз данных и баз знаний [7-11]. Способность систем контроля использовать ИТС определяют эффективность их применения.

Принятие решения о дальнейшей эксплуатации техники осуществляется по двухуровневой шкале: соответствует — не соответствует, на основании обнаружения отклонения от установленного нормативными документами состояния.

Отклонение того или иного параметра от нормы, в качестве которой может выступать диапазон значений или определенное значение измеряемой величины, в соответствии с руководством по эксплуатации, требует ремонта данного технического средства, при этом анализ возможности функционирования данного средства и способности им выполнять требуемый перечень задач и функций, необходимых для данной СТС, средства контроля не проводят и показать не могут. Такие действия должна осуществлять система поддержки принятия решения, входящая в состав системы управления [12, 13].

Современная система предиктивного контроля функционирования СТС требует:

– создания информативных баз данных и баз данных;

– интеграции различных средств контроля и мониторинга СТС, возможности обработки получаемых параметров;

– интеграцию системы контроля в систему поддержки принятия решения и систему управления;

– разработки новых подходов к контролю процесса функционирования системы;

– реализацию процессного рискоориентированного подхода при осуществлении контроля;

– разработку подхода к описанию СТС, позволяющего учитывать процесс функционирования, выполняемые в ней регламенты;

– разработку унифицированных средств контроля для различных СТС, ведомств на основе отечественного оборудования и программного обеспечения;

– автоматизации процесса контроля, формирования сценариев действий по устранению нарушений функционирования системы;

– выявление нарушения функционирования системы на основе анализа функционирования контролируемой системы, изменения характеристик ее функционирования, а также влияния нарушения функционирования отдельных элементов на всю систему и ее элементы.

Таким образом, внедрение систем предиктивного контроля должно привести к уходу от планово-предупредительного обслуживания элементов системы к обслуживанию, реагированию по состоянию элементов системы. Основой системы контроля должна стать информационно-техническая система, функционирование которой осуществляется через взаимодействие баз данных и баз знаний, предназначенных для хранения информации о системе и процессе ее функционирования. Результаты контроля, формируемые в базах знаний и базах данных должны использоваться в системе поддержки принятия решения для обеспечения устойчивого функционирования системы. Основным инструментом для реализации предиктивного контроля предлагается использовать профиль функционирования СТС, характеризующий процесс функционирования системы.

СПИСОК ЛИТЕРАТУРЫ

1. Лепешкин О. М., Ковалев Д. С., Остроумов О. А., Остроумова Е. В. К вопросу о понятии критической информационной инфраструктуры системы управления // I-metods. 2021. № 3. С. 10-15.
2. Михайлов Р. Л., Макаренко С. И. Оценка устойчивости сети связи в условиях воздействия на неё дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы. 2013. № 4. С. 69-79.
3. Бурлов В. Г. Теоретические основы управления риском. СПб.: НПО «Стратегия будущего», 2009. 270 с.
4. Стародубцев Ю. И., Иванов С. А., Закалкин П. В. Концептуальные направления решения проблем обеспечения устойчивости Единой сети электросвязи Российской Федерации в интересах органов государственной власти и военного управления // Военная мысль. 2021. № 4. С. 39-49.
5. Лаута О. С. Метод построения профиля функционирования сложной технической системы / О. С. Лаута, Е. Г. Баленко, В. Х. Федоров [и др.] // Инженерный вестник Дона. 2023. № 2. URL: ivdon.ru/ru/magazine/archive/n1y2023/8183.
6. Остроумов О. А. Модель контроля функционирования системы связи // Известия Тульского государственного университета. Технические науки. 2022. № 3. С. 300-310.
7. Шуравин А. С., Худайназаров Ю. К., Пермяков А. С. Модель сетевого мониторинга распределенной системы управления от внешних сетевых воздействий // Радиолокация, навигация, связь : сб. трудов XXVI Международной научно-технической конференции. Воронеж, 2020. С. 256-261.
8. Коцыняк М. А., Лаута О. С., Нечепуренко А. П. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного противоборства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 1-2 (127-128). С. 58-62.
9. Пермяков А. С., Лепешкин О. М., Митрофанов М. В. Проблемы защищенности информационно-телекоммуникационных сетей специального назначения // Радиолокация, навигация, связь : сборник трудов XXVI Международной научно-технической конференции: в 6 томах. 2020. С. 44-48.
10. Петренко С. А. Концепция поддержания работоспособности киберсистем в условиях информационно-технических воздействий // Труды ИСА РАН. Т. 41. 2009. С. 175-193.
11. Тарасов А. А. Проблема обеспечения гарантоспособности информационных систем и пути ее решения // Системы безопасности, связи и телекоммуникаций. 2000. № 32. С. 78-80.
12. Ларичев О. И., Петровский А. В. Системы поддержки принятия решений: современное состояние и перспективы их развития // Итоги науки и техники. Сер. Техническая кибернетика. М. 1987. Т. 21. С. 131–164.
13. Остроумов О. А., Лепешкин О. М., Синюк А. Д. Систематизация основ методологии синтеза критической информационной инфраструктуры Российской Федерации // Военная мысль. 2021. № 8. С. 109–114.

УДК 621.391.3

АНАЛИЗ СПОСОБОВ СНИЖЕНИЯ ВЛИЯНИЯ ПЕРЕГРУЗКИ КАНАЛОВ И ТРАКТОВ НА ПРОИЗВОДИТЕЛЬНОСТЬ СПЕЦИАЛИЗИРОВАННОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ В ХОДЕ ЕЕ ФУНКЦИОНИРОВАНИЯ

Титов Владимир Степанович, Апарина Елена Юрьевна,
Бабич Борис Иванович, Ащеулов СергейВикторович
Военная академия связи им. Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: Титов856@yandex.ru, elenaaparina.1982@mail.ru, babichbi@mail.ru, asheulov50@mail.ru

Аннотация. В статье проведен анализ способов снижения влияния перегрузки каналов и трактов на производительность специализированной сети передачи данных в ходе ее функционирования, рассмотрены предложения по предотвращению и снижению перегрузки в сети передачи данных и ее элементах.

Ключевые слова: специализированная сеть передачи данных, функционирование сети, управление сетью, перегрузка сети, каналов и трактов.

ANALYSIS OF WAYS TO REDUCE THE IMPACT OF CHANNEL AND PATH CONGESTION ON THE PERFORMANCE OF A SPECIALIZED DATA TRANSMISSION NETWORK DURING ITS OPERATION

TitovVladimr, Aparina Elena, Babich Boris, Ascheulov Sergey
The Millitary Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av., St. Peterburg, 194064, Russia
e-mails: titov856@yandex.ru

Abstract. The article analyzes ways to reduce the impact of channel and path congestion on the performance of a specialized data transmission network during its operation, and considers proposals to prevent and reduce congestion in the data transmission network and its elements.

Keywords: specialized data transmission network, network operation, network management, network overload, channels and paths.

Опыт применения современных телекоммуникационных средств на протоколах общего пользования в вооруженных конфликтах последних лет и в специальной военной операции показывает необходимость их модернизации для обеспечения требований по боевой готовности, живучести, надежности, помехоустойчивости, мобильности, пропускной способности, доступности, разведывательной защищенности и управляемости в сложных и часто меняющихся условиях оперативно-тактической обстановки.

Проектирование и первоначальное развертывание специализированной сети передачи данных (СПД) осуществляется с учетом гарантированного обеспечения рассмотренных сетевых свойств, которые, в свою очередь, определяют своевременность, достоверность и безопасность передачи данных в автоматизированных системах управления войсками и оружием.

Следует отметить, что большинство используемых телекоммуникационных средств общего пользования и специального назначения базируется на протоколы передачи данных и в процессе функционирования нуждаются в устойчивом, непрерывном, оперативном и адекватном управлении ими, при котором еще имеется возможность использования производительности не вышедших из строя автоматических центров (АКЦ), пропускной способности основных каналов и трактов, перераспределения потоков пакетов данных и выполнения вероятностно-временных требований к передаче данных высшей категории срочности.

В таких ситуациях могут быть применены соответствующие способы управления внешней (поступающей в сеть) и внутренней (функционирующей в сети) нагрузкой, а также использованы резервные средства и комплексы, каналы и линии связи (при их наличии) с адаптивным изменением режимов их работы.

Общий принцип эффективности адаптивного управления нагрузкой приведен в [1] на примере анализа зависимости производительности СПД по скорости передачи пакетов данных $R_{\text{п}}$ от входной нагрузки $R_{\text{вх}}$, определяемой количеством поступающих пакетов и качеством управления нагрузкой.

Идеальным случаем является оптимальное управление нагрузкой, когда обеспечивается ввод в сеть и передача всех пакетов до достижения порогового значения пропускной способности $C = max\,(R_{\text{п}})$, а затем величина $R_{\text{п}}$ не изменяется. Это характеризует возможную потерю части поступивших пакетов данных $R_{\text{пот}} = C - R_{\text{п}}$., характерную для СПД с применением телекоммуникационных средств общего пользования [2].

Для специализированных сетей передачи данных вводятся ограничения по вероятности потери пакетов данных. В ряде случаев нормируется вероятность недоведения пакетов данных, связанная непосредственно или косвенно (по количеству транзитов в маршруте передачи) с временем старения данных [3, 4].

На практике, при увеличении входной нагрузки выше определенного значения, пропускная способность снижается $R_{\text{пер}} < C$. С этого момента сеть передачи данных и ее элементы переходят в состояние перегрузки, когда степень снижения пропускной способности зависит от качества и способов управления нагрузкой. При этом реальная пропускная способность сети без управления значительно ниже пропускной способности и может

увеличена применением различных способов глобального управления в масштабе всей сети и локального управления для отдельных ее зон, а также для центров коммутации [2].

Достоинством централизованного управления является возможность обеспечения оптимального управления нагрузкой по информации о состоянии сети передачи данных в целом. Однако для сбора и обработки этой информации требуется достаточно большое время, дополнительный канальный ресурс и высокопроизводительные вычислительные средства. Невыполнение этих требований и отсутствие достаточной статистики снижает эффективность принятого решения для отдельных элементов сети передачи данных, в которых будет наблюдаться состояние перегрузки.

Перегрузка может быть вызвана различными факторами на различных элементах сети. Следует различать потоки пакетов данных, поступающих в АКЦ со стороны оконечного оборудования данных и потоки пакетов данных от смежных АКЦ. Для этого в памяти АКЦ организуются соответствующие очереди по различным дисциплинам обслуживания с учетом приоритетов обслуживания и категорий срочности [2, 3].

При полном заполнении памяти, ограниченной по объему, вновь прибывающие пакеты могут быть потеряны. Увеличение объема памяти АКЦ при низкой производительности вычислительных средств, некорректности сетевого программного обеспечения, использования низкоскоростных каналов и каналов с высоким уровнем помех не может обеспечить значительное снижение функционирующей нагрузки в СПД.

Например, низкая производительных вычислительных средств АКЦ является причиной перегрузки за счет сравнительно больших затрат процессорного времени при реализации процедур учета поступающих, принятых и переданных пакетов данных, их категорийной и приоритетной обработки и маршрутизации. При этом очередь может появиться и лавинообразно увеличиваться даже при достаточной пропускной способности каналов и линий связи.

На предотвращение перегрузки сетевых элементов существенное влияние оказывает выбор исходного алгоритма маршрутизации пакетов и сообщений на сетевом и транспортном уровнях и возможность его адаптивного функционирования при передаче данных по сети.

Характер увеличения функционирующей нагрузки в сети и заполнения буферной памяти существенно зависит как от ограничений на количество повторных передач пакета данных, на который отсутствует подтверждение о приеме, так и от «ширины окна», в котором предусмотрено подтверждение на группу из нескольких пакетов (кадров, линейных или сетевых блоков).

В качестве примера можно привести результаты исследований сетевого протокола общего пользования X.25, который в обычных условиях функционирования считается надежным и помехоустойчивым [2, 3]. Исследования показали, что в зависимости от критического состояния сети и поступающей нагрузки следует снизить «ширину окна» до одного пакета, а количество повторных передач и используемых альтернативных маршрутов не более трех [5].

Заслуживают внимания и различные способы управления очередями, особенности которых рассмотрены в [2, 3] для телекоммуникационных сетей общего пользования и учитывающие приоритетность передаваемых данных.

Следует отметить, что на предотвращение перегрузки сети и снижение функционирующей нагрузки оказывает влияние управление временем жизни пакетов по количеству транзитов в маршруте передачи. При большом числе транзитов нагрузка на сеть пропорционально увеличивается. Однако, если время жизни пакета слишком мало, то потерянные по различным причинам пакеты не будут успевать достичь адресата, что приведет к необходимости их повторных передач и неоправданному увеличению функционирующей нагрузки, снижению производительности АКЦ и пропускной способности каналов и трактов передачи данных.

На транспортном уровне применяются аналогичные методы управления поступающей и функционирующей нагрузкой с учетом особенностей использования в качестве исходных данных времени пакетной передачи сообщения в целом, так как время передачи каждого пакета в сети носит случайный характер. При этом можно использовать результаты, полученные при использовании эхо-протокола на основе процедуры ping для сетей передачи данных общего пользования. В специализированных сетях для этой цели обычно используют вызывные и ответные сообщения в защищенном формате.

В ряде случаев в качестве способов для снижения влияния перегрузки каналов и трактов на производительность специализированной сети передачи данных в ходе ее функционирования могут быть использованы многоуровневые протоколы управления передачей данных из семейства ЕСПИО, учитывающие предназначение и особенности функционирования специализированных сетей передачи данных, относительные и абсолютные приоритеты передаваемых данных по их категориям срочности [6, 7].

СПИСОК ЛИТЕРАТУРЫ

1. Теоретические основы передачи данных : уч. пособие. / под ред. В. С. Титова. СПб.: ВАС, 2013. 212 с.
2. Олифер В, Олифер Н. Компьютерные сети. Принципы, технологии, протоколы : юбилейное изд. СПб.: Питер, 2020. 1008 с.
3. Умрихин Ю. Д. Адаптивная маршрутизация и контроль перегрузок в сетях передачи и распределения информации // Автоматы и управление: процессы и устройства управления в сетях связи. М.: Наука, 1982. С. 86-109.
4. Устройство децентрализованного управления распределением пакетов сообщений в сети передачи данных: пат. РФ № 2213427; заяв. № 2002111502/09 от 29.04.2002 г. / В. С. Титов, И. Я. Бурнашев, И. А. Нестеров, А. Г. Романов, Г. В. Шарко.
5. Способ управления потоками данных в центрах коммутации при сопряжении разнородных сетей: пат. РФ № 2369028; заяв. № 2007134482 от 14.09.2007 г. ; опубл. 27.09.2009 / В. С. Титов, В. А. Королев, В. Е. Поносов, П. Г. Романенко.
6. Титов В. С., Сазонов В. В., Ионников А. С. Адаптация системы передачи информации к условиям ведения радиоэлектронной борьбы // Актуальные проблемы защиты и безопасности. Труды XVIII Всероссийской научно-практической конференции РАРАН, 1-4 апреля 2015 г. СПб.: ВУНЦ ВМФ Военно-морская академия им Н. Г. Кузнецова, 2015. Т. 5. С. 189-192.
7. Титов В. С., Зубакин В. В., Сазонов В. В. Вариант планирования и подготовки к функционированию сети передачи данных соединения // Научно-технический сборник № 98. СПб.: ВАС, 2017. С. 47-54.

УДК 004.654

ПРИМЕНЕНИЕ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ СЕТЕЙ ДЛЯ СИНХРОНИЗАЦИИ БАЗ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Удальцов Александр Владимирович, Саенко Игорь Борисович
Военная академия связи имени Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: axil2003@yandex.ru, ibsaen@mail.ru

Аннотация. Рассматривается применение генеративно-состязательных сетей для синхронизации баз данных. Обучение таких сетей на реальных данных и генерация новых данных позволяют достичь синхронизации баз данных с высокой степенью актуальности информационных ресурсов. Предлагается использовать такие сети для синхронизации на основе SQL-запросов, определяя, какие запросы изменяют данные в базе данных и требуют синхронизации. Это подход позволяет улучшить эффективность и надежность синхронизации баз данных в информационных системах.

Ключевые слова: генеративно-состязательная сеть, информационный ресурс, базы данных, синхронизация баз данных.

APPLICATION OF GENERATIVE ADVERSARIAL NETWORKS FOR DATABASE SYNCHRONIZATION IN SPECIAL-PURPOSE INFORMATION SYSTEMS

Udal'tsov Alexander, Saenko Igor
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails: axil2003@yandex.ru, ibsaen@mail.ru

Abstract. The application of generative adversarial networks for database synchronization is considered. The training of such networks on real data and the generation of new data make it possible to achieve synchronization of databases with a high degree of relevance of information resources. It is proposed to use such networks for synchronization based on SQL queries, determining which queries change the data in the database and require synchronization. This approach improves the efficiency and reliability of database synchronization in information systems.

Keywords: generative adversarial networks, information resource, databases, database synchronization.

Синхронизация баз данных является важной составляющей для работы информационных систем, обеспечивающим актуальность данных. Существующие методы синхронизации баз данных имеют ограничения и сложности, такие как распределённость информационных ресурсов и сложность настройки. В последние годы генеративно-состязательные сети (GAN) привлекли большое внимание и показали потенциал в различных областях, в том числе в информационных системах специального назначения. Использование GAN при синхронизации баз данных может привести к новым инновационным решениям в области информационных систем.

К информационным ресурсам относят всю совокупность данных, организованных для эффективного получения достоверной информации в интересах обеспечения бесперебойного функционирования информационной системы [1].

Сети GAN представляют собой класс глубоких нейронных сетей, которые применяются для генерации новых данных, имитации распределения существующих данных, связанных с моделированием и синтезом. Они состоят из двух основных компонентов: генератора и дискриминатора. Генератор отвечает за создание новых образцов данных, имитируя существующие или генерируя совершенно новые. Он обучается на основе обучающей выборки и стремится создать данные, которые неотличимы от реальных. Дискриминатор же выполняет роль классификатора и старается отличить сгенерированные данные от реальных. Обучение GAN происходит через состязание между генератором и дискриминатором, где они взаимодействуют и совершенствуются, пока не достигнут оптимального баланса [2].

Применение GAN представляет собой новый подход к решению проблемы синхронизации баз данных. Сети GAN могут быть использованы для генерации и синхронизации данных между несколькими базами данных, обеспечивая их целостность и актуальность. Путем обучения GAN на реальных данных и последующего генерирования новых данных можно достичь синхронизации данных, у которых расхождения между базами данных будет минимальна. Использование GAN для синхронизации баз данных в информационных системах может привести к повышению эффективности и надежности синхронизации и, как следствие, актуальности данных, которые будут использоваться, например, в системах поддержки принятия решений.

Для использования GAN необходимо провести анализ баз данных. Для этого необходимо изучить типы связей и структуру базы данных. Это необходимо для того, чтобы выбрать подходящую структуру GAN. Для работы GAN необходимо сформировать обучающею выборку, которая будет включать синхронизированные информационные ресурсы. Предварительно информационные ресурсы преобразуются в формат, пригодный для обучения GAN.

В докладе рассматривается простой пример использования GAN для синхронизации баз данных. Предположим, что у нас есть множество SQL-запросов к базе данных. Они могут быть предназначены для добавления новых записей, обновления или удаления существующих записей и чтения записей. Запросы производят изменения в базе данных и требуют синхронизации с остальными связанными базами данными.

Необходимо определить, какие SQL-запросы будут менять данные, а какие нет. Необходимо научить GAN распознавать запросы, которые изменяют данные в базе данных, и давать команду на синхронизацию этих данных в связанных базах данных. Для этого необходимо сгенерировать запросы с использованием GAN, которые имитировали бы изменения реальных данных. При наличии реальных и сгенерированных запросов GAN может определять, какие данные должны быть изменены, а также можно проверить, будет ли обеспечена актуальность и целостность данных [3].

Таким образом, можно сделать вывод о том, что использование GAN для определения необходимости синхронизации информационных ресурсы позволяет повысить актуальность информационных ресурсов и более эффективно настраивать синхронизацию баз данных в сложных информационных системах.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И. В., Саенко И. Б., Паращук И. Б. Критерии оценки доступности информационных, телекоммуникационных и других критически важных ресурсов в интересах анализа их защищенности // Региональная информатика и информационная безопасность. XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 2021 : сб. трудов. Вып. 10. С. 97-101.
2. Саенко И. Б., Котенко И. В. Генетическая оптимизация и визуальный анализ при формировании схем доступа в ВЛВС // Информационные технологии и вычислительные системы. 2015. № 1. С. 33-46.
3. Андриян И. В., Андриян О. В Принцип работы и методы обучения генеративно-состязательных нейросетей // Наука и современность: материалы Всероссийской научно-практической конференции студентов и молодых ученых, Таганрог, 12 ноября 2021 г. Таганрог : ЭльДирект : ИП Шкуркин Д. В. (ДиректСайнс), 2021. С. 72-74. EDN ZAPPWI.

УДК 004.056.53

ПОДХОД К ОБНАРУЖЕНИЮ И АВТОМАТИЧЕСКОЙ КЛАССИФИКАЦИИ НЕСАНКЦИОНИРОВАННЫХ ВОЗДЕЙСТВИЙ НА ИНФОРМАЦИОННУЮ ТЕЛЕКОММУНИКАЦИОННУЮ СИСТЕМУ

Усов Николай Александрович, Филимонов Василий Александрович, Остроумов Олег Александрович
Военная академия связи имени Маршала Советского Союза С. М. Буденного,
Тихорецкий пр, 3, Санкт-Петербург, 194064, Россия
e-mails: nauvrn@rambler.ru, awgn@yandex.ru, oleg-26stav@mail.ru

Аннотация. В докладе рассматривается способ достижения заданного показателя выявления несанкционированных воздействий на информационную телекоммуникационную систему, основанный на переборе вариантов структур обнаружителей. Показано, что для реализации основных процедур предлагаемого способа целесообразно использование нейросетевых технологий. Обоснован вариант технической реализации устройства, обеспечивающего не только эффективное обнаружение несанкционированных воздействий, но и возможность их автоматической классификации.

Ключевые слова: информационная телекоммуникационная система, несанкционированное воздействие, информационная угроза, технический канал утечки информации, нейросетевые технологии, классификация.

APPROACH TO DETECTION AND AUTOMATIC CLASSIFICATION OF UNAUTHORIZED IMPACTS ON INFORMATION TELECOMMUNICATION SYSTEM

Usov Nikolay, Philimonov Vasiliy, Ostroumov Oleg
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny,
3 Tikhoretsky Pr, St. Petersburg, 194064, Russia
e-mails: nauvrn@rambler.ru, awgn@yandex.ru, oleg-26stav@mail.ru

Abstract. The report discusses a way to achieve a given indicator for detecting unauthorized impacts on an information telecommunication system based on a search of variants of detector structures. It shown that is advisable to use neural network technologies to implement the basic procedures of the proposed method. A variant of the device technical implementation providing not only effective detection of unauthorized impacts, but also the possibility of their automatic classification is substantiated.

Keywords: information telecommunication system, unauthorized impact, information threat, technical channel of information leakage, neural network technologies, classification.

На сегодняшний день информационные телекоммуникационные системы (ИТКС) играют важную роль в обеспечении процесса функционирования государственных и военных структур. Повсеместное использование вычислительных систем для хранения, обработки и передачи информации делает чрезвычайно важными проблемы их защиты, особенно учитывая глобальную тенденцию к росту числа информационных угроз, реализуемых посредством несанкционированных воздействий различного рода. В большинстве практически важных случаев такие воздействия приводят к существенному снижению эффективности деятельности структур, применяющих ИТКС, а также к значительным материальным (финансовым) потерям.

При этом под угрозой оказываются интересы безопасности Российской Федерации, экономическая безопасность предприятий и организаций (фирм), физическая безопасность человека, его права и свободы, а также материальные и духовные ценности общества.

В этой связи весьма своевременными, важными и актуальными будут исследования, направленные на разработку эффективных способов исключения технических каналов утечки информации в ИТКС путем выявления и нейтрализации несанкционированных воздействий и обоснование структуры технических средств для их реализации.

Рациональным представляется способ выявления несанкционированных воздействий на ИТКС, предполагающий вычисление время-стоимостной матрицы для всех возможных вариантов структуры обнаружителя при обнаружении каждого классифицированного несанкционированного воздействия, определение на основе элементов матрицы показателя обнаружения того или иного воздействия конкретным обнаружителем и сравнение данного показателя с эталоном.

Рассматриваемый способ в случае его аппаратной реализации будет весьма дорогостоящим, трудоемким и затратным по времени.

По этой причине стоит обратить внимание на программную реализацию предложенных процедур. Кроме того, одними из наиболее перспективных будут способы выявления несанкционированных воздействий с применением нейросетевых технологий [1-2].

Однако известные к настоящему времени технические средства, обеспечивающие выявление несанкционированных воздействий различного характера на информационные телекоммуникационные системы (например, нейронная сеть типа многослойный персептрон [1–3], устройство выявления вредоносных программ (компьютерных вирусов) [4–5] и др.), характеризуются рядом недостатков, среди которых наиболее существенными являются выявление всего одного класса несанкционированных воздействий и ограничение числа разновидностей воздействий внутри класса.

Устранение перечисленных недостатков требует обоснования технического облика устройства выявления несанкционированных воздействий на информационную телекоммуникационную систему, обеспечивающего решение задачи выявления новых классов подобных воздействий. При этом должны быть сняты жесткие ограничения на количество обнаруживаемых классов несанкционированных воздействий.

Здесь сущность технического решения заключается в сравнении анализируемых несанкционированных воздействий с заданными классами, выявлении новых классов несанкционированных воздействий и их учете в процессе дальнейшей классификации.

Структурная схема варианта устройства выявления несанкционированных воздействий на ИТКС включает устройство ввода информации, сумматор, преобразователь кода, блоки ключей, блок детекторов, блок сравнения, логический элемент, классификатор и базу данных классов воздействий.

Проведенные исследования позволили добиться ряда важнейших преимуществ, основными из которых являются:

– относительная простота технической реализации предложенного устройства может обеспечить его конструирование в короткие сроки за счет использования существующей элементной базы, а также известных программных и аппаратных узлов и блоков;

– возможность расширения классификации несанкционированных воздействий по факту обнаружения неизвестных классов НСВ при одновременном их запоминании в базе данных (классов);

– снятие ограничений на количество обнаруживаемых классов воздействий;

– универсальность структурной схемы устройства;

– инвариантность процесса функционирования устройства выявления НСВ на ИТКС, позволяющая принципиально выявлять любые воздействия применительно к любым ИТКС.

СПИСОК ЛИТЕРАТУРЫ

1. Хайкин С. Нейронные сети: полный курс / пер. с англ. под ред. Н. Н. Куссуль. М.: Издательский дом «Вильямс», 2006. 1104 с.
2. Осовский С. Нейронные сети для обработки информации / пер. с польского И. Д. Рудинского. М.: Финансы и статистика, 2002. 344 с.
3. Круглов В. В., Борисов В. В. Искусственные нейронные сети. Теория и практика. М.: Горячая линия-Телеком, 2002. С. 53-58.
4. Bezobrazov S. Neural networks and artificial immune systems — malware detection tool // OWD: proceedings of the X International PhD Workshop. Gliwice, 2008. Pp. 465-469.
5. Bezobrazov S. Artifical immune system approach for malware detection: neural networks applying for immune detectors construction // International journal of «Computing». 2008. Vol. 7. № 2. P. 44-50.

УДК 621.396.4

ОБЩИЙ ПОДХОД К ДЕМОДУЛЯЦИИ СИГНАЛОВ С ЦИФРОВОЙ ФАЗОВОЙ МОДУЛЯЦИЕЙ В СИСТЕМАХ СВЯЗИ ДЕКАМЕТРОВОГО ДИАПАЗОНА

Филимонов Василий Александрович, Усов Николай Александрович, Остроумов Олег Александрович
Военная академия связи имени Маршала Советского Союза С. М. Буденного,
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: nauvrn@rambler.ru, awgn@yandex.ru, oleg-26stav@mail.ru

Аннотация. В условиях санкций со стороны «недружественных» стран и введения ими запрета на технологическое оборудования остро встает вопрос о замене ее отечественными разработками. При разработке новых образцов техники необходимо произвести анализ уже разработанного оборудования. Анализ должен подразумевать в себе не только технические характеристики, но и алгоритмы работы, заложенные в этом оборудовании. В докладе рассматривается задача создания (раскрытия, заложенных авторами протоколов) алгоритмов демодуляции сигналов с цифровой фазовой модуляцией на примере декаметровой телекоммуникационной системы авиации (HFDL) разработанной корпорацией ARINC. Рассмотрена структура передаваемого кадра. Выделены отдельные последовательности преамбулы и указаны их назначения. Более

подробно рассмотрены варианты коррекции принимаемых информационных символов, искаженных в результате прохождению сигнала через канал связи. Указаны наиболее вероятные подходы коррекции принятых символов.

Ключевые слова: декаметровые системы связи, HFDL, коррекция канала связи, сигналы PSK, М-последовательности, импульсная характеристика канала связи.

GENERAL APPROACH TO SIGNALS DEMODULATION WITH DIGITAL PHASE MODULATION IN THE HIGH FREQUENCY COMMUNICATION SYSTEMS

Usov Nikolay, Philimonov Vasiliy, Ostroumov Oleg
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny,
3 Tikhoretsky Pr, St. Petersburg, 194064, Russia
e-mails: nauvrn@rambler.ru, awgn@yandex.ru, oleg-26stav@mail.ru

Abstract. In the context of «unfriendly» countries sanctions and their ban introduction on technological equipment, the question of replacing it with domestic developments is acute. When developing new models of equipment, it is necessary to analyze the already developed equipment. The analysis should include not only technical characteristics, but also the operation algorithms embedded in this equipment. The report considers the task of creating (disclosing the protocols laid down by the authors) algorithms for demodulating signals with digital phase modulation using the decameter aviation telecommunication system (HFDL) developed by the ARINC corporation as an example. The structure of the transmitted frame is considered. Separate sequences of the preamble are singled out and their purposes are indicated. The options for correcting received information symbols distorted as a result of the signal passing through the communication channel are considered in more detail. The most probable approaches for correcting the received symbols are indicated.

Keywords: HF communication system, HFDL, correct channels, signal PSK, M-sequence, impulse response channel.

В условиях санкций со стороны «недружественных» стран и введения ими запрета на технологическое оборудования, остро встает вопрос замены его отечественными разработками. Не секрет, что многие разработки доведены до уровня микросхем (чипов) и тем самым заложенные в них алгоритмы не подлежат «извлечению». Таким образом, информационная безопасность страны состоит не только в защите от воздействия «противником» на информационные потоки, но и от скорейшего создания отечественных телекоммуникационных систем. При этом разработка отечественных систем связи должна касаться всех уровней эталонной модели взаимодействия открытых систем (ЭМВОС) включая физический и канальный уровень. Необходимо отметить, что ряд телекоммуникационных систем, которые используются в международных (глобальных) проектах невозможно заменить полностью отечественными системами. В данных системах необходимо переходить только на отечественную элементную базу, при этом алгоритмы функционирования должны остаться прежними. Примером таких систем может служить декаметровая автоматическая телекоммуникационная система авиации (HFDL) разработанная корпорацией ARINC [1]. Стоит отметить, что во многих случаях не только алгоритмы, но протоколы работы телекоммуникационных систем являются закрытыми.

Анализ нижних уровней ЭМВОС данной системы позволяют сделать вывод о стандартном построении этой системы при использовании сигналов PSK-2, 4 и 8. Между тем имеются ряд особенностей связанные с тем, что корреспондентами системы являются самолеты, имеющие большие скорости перемещения, следовательно, обладающие большим доплеровским эффектом. Для борьбы с этим эффектом стандартом предусматривается передача одного тона перед началом кадра передачи данных, что значительно облегчает осуществление частотной синхронизации на первоначальном этапе.

Наибольший интерес представляет демодуляция передаваемых данных. В этом стандарте данные, подлежащие передачи разбиваются на блоки длительностью 30 символов PSK-2, 4 или 8 в зависимости от выбранной скорости передачи. После передачи преамбулы каждый блок данных заканчивается передачей 15-ти элементной М-последовательностью символов PSK-2. Заключительная часть преамбула содержит девять таких же 15-ти элементных М-последовательностей. Таким образом, каждый блок данных окружен известными символами. Такая структура позволяет оценивать быстроизменяющиеся характеристики канала связи. Только этим можно объяснить, что в передаваемом кадре информационных символов, т.е. собственно данных, содержится меньше половины.

Передаваемые через каждые 30 символов известные и одинаковые символы PSK-2 (повторяющиеся последовательности) позволяют оценивать изменение частотного ухода [2]. Пример использования этого алгоритма представлен в [3].

Вариант оценивания частоты ухода на каждом передаваемом блоке, несомненно дает определенные преимущества. Однако, необходимо исследовать насколько объективна будет эта оценка в каналах с межсимвольной интерференцией (МСИ). Тем не менее, можно объективно отметить, что для данных каналов связи модель Ваттерсона [4] в прямом виде не применима.

Принятые сигнальные символы можно рассмотреть как свёртку передаваемых символов PSK с импульсной характеристики (ИХ) канала связи.

Учитывая, что характеристики канала связи постоянно изменяются, корректировку ИХ канала связи необходимо производить на каждом принятом блоке. В этом случае считается, что на его длительности ИХ канала не изменяется, т.е. канал связи стационарен.

Коррекцию принятых символов можно производить по основному лучу или использовать все искаженные символы, т.е. всю ИХ канала связи. Можно предположить, что коррекция, учитывающая всю длину ИХ канала связи, даст более правильное решение о принятом символе. Однако, для этого необходимо, чтобы рассчитываемая длина ИХ совпадала или была больше реальной.

Наиболее широко описанный способ коррекции принятых символов связан с адаптивной фильтрацией [5]. Адаптивная фильтрация, в общем случае успешно справляются с коррекцией канала связи, если изменения условий приема сигнала происходят не слишком быстро, когда фильтр успевает пересчитать свои коэффициенты и перейти в новое состояние. Для конкретного протокола, необходимо учитывать не только ограниченность первоначальной известной последовательности, но короткие известные последовательности, служащие в этом случае для перерасчета коэффициентов фильтра. Используемый алгоритм LMS показал не очень хорошие результаты сходимости алгоритма при работе на реальном сигнале.

Наиболее подходящим, по мнению авторов, является вычисление ИХ канала связи на каждом блоке по двум окружающим его известным последовательностям с усреднением результатов расчетов. Нахождение ИХ канала связи по известным последовательностям описано в [3]. Правильность данного подхода показывает нахождение обратной матрицы на основе 15-ти элементной М-последовательности.

Коррекция символов информационного блока по рассчитанной ИХ канала связи с использованием БПФ в настоящее время находится в разработке.

Таким образом, можно с большой долей уверенности утверждать, что, демодуляция сигнала декаметровой телекоммуникационной системе авиации (HFDL) осуществляется путем деления на блоки по 60 символов из которых первые и последние 15 символов являются известными на приеме М-последовательностями и 30 неизвестными, являющимися информационными и подлежащими демодуляции. Демодуляция (принятие решения о переданном символе) информационной части блока осуществляется после коррекции принятой последовательности, на основе рассчитанной ИХ канала связи.

Рассмотренный подход обладают универсальностью, так как при рассмотрении других протоколов систем связи декаметрового диапазона обнаруживается сходство блокового построения и существование обратных матриц необходимых для вычисления ИХ канала связи.

СПИСОК ЛИТЕРАТУРЫ

1. Aeronautical telecommunications. International Standards and Recommended Practices and Procedures for Air Navigation Services. Montreal: ICAO. 2001.
2. Nezami M. K. RF Architectures and Digital Signal Processing Aspects of Digital Wireless Transceiver. 2003. 513 c.
3. Филимонов В. А. Теория электрической связи через цифровую обработку сигналов с примерами в MATLAB : учеб. пособие. М. ; Вологда : Инфра-Инженерия, 2022. 780 с.
4. Recommendation ITU-R 520-2. Use of high frequency ionospheric channel simulators [Электронный ресурс]. URL: https://www.itu.int/rec/R-REC-F.520-2-199203-W/en (дата обращения: 30.06.2023).
5. Уидроу Б., Стирнз С. Адаптивная обработка сигналов / пер. с англ. М.: Радио и связь. 1989. 440 с.

УДК 004.6:004.7

ПРИМЕНЕНИЕ РАСПРЕДЕЛЕННОЙ ВИРТУАЛЬНОЙ МАШИНЫ ДЛЯ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ СЕНСОРНОЙ СЕТИ

Шальнев Илья Олегович
СПИИРАН – СПб ФИЦ РАН
14 линия, 39, Санкт-Петербург, 199178, Россия
e-mail: shalnev.i@iias.spb.su

Аннотация. Рассматривается подход к построению сенсорной сети с использованием коммуникационной инфраструктуры на основе распределенной виртуальной машины.

Ключевые слова: сенсорная сеть; виртуальная машина; распределенная обработка данных.

INCREASING THE SECURITY OF A SENSOR NETWORK BY USING A DISTRIBUTED VIRTUAL MACHINE

Shalnev Ilia
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line St, Petersburg, 199178, Russia
e-mails: shalnev.i@iias.spb.su

Abstract. An approach to building a sensor network using a communication infrastructure based on a distributed virtual machine is considered.

Keywords: sensor network; virtual machine; distributed data processing.

Сенсорные сети представляют собой распределенные сети устройств, которые могут быть использованы в различных областях, таких как мониторинг окружающей среды, управление инфраструктурой, сельское хозяйство, здравоохранение, автомобильная промышленность и многих других. Узлы таких сетей, называемые датчиками или сенсорами, используются для мониторинга различных параметров, таких как температура, влажность, уровень шума, движение и многое другое.

Большое распространение сенсорных сетей показывает их востребованность и большой потенциал к решению многих задач [1, 2], но также и уязвимость к при наличии у злоумышленника физического доступа к узлам сенсорной сети.

Задача взаимодействия в современных распределенных киберфизических и вычислительных системах многократно решалась применительно к конкретной прикладной задаче, но единого универсального способа разработки программного обеспечения (ПО) для таких систем до сих пор не существует. Это связано с тем, что расширение области решаемой задачи требуют модификации протокола межузловой коммуникации, а любые модификации протокола, в свою очередь, требуют обновления программного обеспечения на всех узлах системы.

Архитектура и состав комплекса программных библиотек для реализации взаимодействия в распределенных системах на основе коммуникационной среды, организованной в виде распределенной виртуальной машины [3, 4]. Данная модель взаимодействия между вычислительными узлами в распределенной сети основана на передачи информации в виде последовательности вызовов функций распределённых программных объектов, что с одной стороны позволяет снизить объем передаваемых данных и временные затраты на обработку передаваемой информации. При этом предполагается, что распределённая система должна разрабатываться как единая программа, в которой взаимодействие изолированных программных компонентов синтаксически схоже с организацией взаимодействия в классическом приложении. Узлы распределённой системы должны рассматриваться не по отдельности, а как единый вычислительный ресурс [5].

Динамический характер распределения задач между узлами распределенной системы дает повышение безопасности сенсорной сети за счет того, что в случае утери или перехвата одного из узлов системы не даст возможность копирования с него ПО, так как весь функционально-значимый исполнимый код передается на устройство динамически непосредственно перед его выполнением.

Таким образом, описанный подход к построению сенсорной сети с использованием коммуникационной инфраструктуры на основе распределенной виртуальной машины может быть эффективно использован для обеспечения безопасности узлов сети за счет отсутствия хранимого программного кода, хранящегося на узлах сети, в том числе на узлах-сенсорах.

СПИСОК ЛИТЕРАТУРЫ

1. Multi-Layered Mobile Sensor Network With Robot Team [Электронный ресурс]. URL: http://dx.doi.org/10.1115/imece2005-81438 (дата обращения: 30.09.2023).
2. Design and Research of Intelligent Warehouse Monitoring System of Multimedia Sensor Network [Электронный ресурс]. URL: http://dx.doi.org/10.4028/www.scientific.net/amm.713-715.637 (дата обращения: 30.09.2023).
3. Кулешов С. В., Шальнев И. О. Особенности реализации распределенной виртуальной машины при построении коммуникационной инфраструктуры общего назначения // Изв. вузов. Приборостроение. 2023. № 2.
4. Шальнев И. О. Подход к построению распределенной виртуальной машины на основе объектно-ориентированного программирования // Известия тульского государственного университета технические науки. Вып. 9. 2020, с. 40-47.
5. Кулешов С. В., Зайцева А. А., Шальнев И. О. Подход к реализации распределенной системы виртуальных машин для самоорганизующихся сетей // Информационно-управляющие системы. 2019. № 5 (102). С. 30-37.

УДК 621.396.4

ЗАДАЧИ СИНТЕЗА ТОПОЛОГИЧЕСКОЙ СТРУКТУРЫ СЕТИ ПЕРЕДАЧИ ДАННЫХ С УЧЕТОМ ПАРАМЕТРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Шинкарев Семен Александрович, Паращук Игорь Борисович
Военная академия связи имени Маршала Советского Союза С.М. Буденного,
Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия
e-mails: se_men82@mail.ru, shchuk@rambler.ru

Аннотация. В докладе на основе анализа требований, тенденций развития сетей передачи данных, условий их функционирования и требований к их защищенности, сформулированы общие задачи синтеза структуры сетей такого класса с учетом показателей информационной безопасности. Этот подход представляет собой последовательность решаемых многокритериальных оптимизационных задач в комбинаторном пространстве допустимых безопасных топологических структур. Обоснован выбор целевых функций, являющихся основными сетевыми характеристиками и характеристиками информационной безопасности сетей передачи данных. Предложено решение данных задач осуществлять на основе декомпозиции общей задачи синтеза на ряд взаимоувязанных подзадач формирования топологической, потоковой и физических структур.

Ключевые слова: сети передачи данных, топологическая структура, синтез, параметры информационной безопасности, теория графов.

TASKS OF SYNTHESIS OF THE TOPOLOGICAL STRUCTURE OF THE DATA TRANSMISSION NETWORK TAKING INTO ACCOUNT THE PARAMETERS OF INFORMATION SECURITY

Shinkarev Semyon, Parashchuk Igor
Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny
Tikhoretsky Ave., 3, St. Petersburg, 194064, Russia
e-mails: se_men82@mail.ru, shchuk@rambler.ru

Abstract. In the report, based on the analysis of requirements, trends in the development of data transmission networks, the conditions of their functioning and the requirements for their security, the general tasks of synthesizing the structure of networks of this class, taking into account information security indicators, are formulated. This approach is a sequence of solved multi-criteria optimization problems in the combinatorial space of permissible safe topological structures. The choice of target functions, which are the main network characteristics and characteristics of information security of data transmission networks, is justified. The solution of these problems is proposed to be carried out on the basis of decomposition of the general synthesis problem into a number of interrelated subtasks of the formation of topological, flow and physical structures.

Keywords: data transmission networks, topological structure, synthesis, information security parameters, graph theory.

Синтез топологической структуры с учетом параметров информационной безопасности является первым и главным этапом построения сетей передачи данных (СПД), он проводится для снижения топологической неопределенности, повышения структурной надежности и защищенности сетей такого класса [1, 2].

Характеристики топологической структуры определяют показатели функционирования и показатели безопасности СПД, возможности по управлению, реконфигурированию, развитию, наращиванию, приведенной стоимости, использованию альтернативных путей доступа, предотвращению вторжений и т.п. Поэтому весьма важно уже на первоначальном этапе построения сети синтезировать оптимальную (рациональную) топологическую структуру (ТС) с учетом параметров информационной безопасности (ПИБ) [3].

Под синтезом ТС с учетом ПИБ понимается определение числа и местоположения узлов и построение сетки линий сети, отвечающих предъявляемым требованиям к надежности, живучести и информационной безопасности направлений связи. Полученное на этапе ТС решение будет являться допустимым и позволяет в последующем реализовать необходимый ресурс по пропускной способности, качеству, помехоустойчивости и защищенности СПД [4, 5].

Рассмотрим содержание этапов синтеза структуры СПД с учетом ПИБ. Формализация задачи синтеза топологической структуры СПД с учетом ПИБ, в самом общем виде, может быть представлена путем определения целевых функций и зависимостей между множеством возможных принципов построения СПД и ее элементов, множеством взаимосвязанных функций, выполняемых сетью, множеством целей функционирования сети и множеством взаимосвязанных элементов СПД при выполнении заданных ограничений.

Являясь частью системы, топологическая структура должна оцениваться по тем же критериям, что и сама СПД, кроме того, желательно установить аналитические соотношения между их характеристиками качества и информационной безопасности. Однако данный подход не реализуем для таких сложных систем как региональные сети, поскольку значения критериев системы невозможно вычислить с достаточной точностью на ранних этапах синтеза, а также не существует универсальных методик формального перехода от сетевых характеристик СПД к топологическим характеристикам [5].

Топологическая структура сети связи представляет собой совокупность узлов и соединяющих их линий в их взаимном расположении. Мощным средством исследования сетей связи является математический аппарат теории графов [6-9].

Требования к характеристикам топологической структуры сети, то есть требования к параметрам графа, представляющего СПД с учетом ПИБ: неиерархичность по отношению к системам управления; минимально возможное среднее расстояние на сети; требуемая связность, требуемая информационная безопасность и максимальное число остовных деревьев; доступность ресурса сети в требуемом объеме из любого узла сети; возможность реконфигурирования, наращивания сети без значительных капитальных затрат, а также близкая к минимальной приведенная стоимость реализации.

Наиболее полно данным требованиям удовлетворяет класс графов с экстремальными значениями таких параметров как защищенность, диаметр, среднее расстояние и число остовных деревьев.

Представим топологическую структуру СПД в виде связного неориентированного графа без петель и кратных ребер, причем учитываются множество элементов сети, таких как: коммутаоры (сетевые элементы); контроллеры; множество линий, соединяющих узлы сети (ребра графа).

Тогда синтез топологической структуры СПД с учетом ПИБ представляет собой выбор, или выделение из всей совокупности графов некоторого подмножества, которое наилучшим способом соответствует принципам построения и целям функционирования сети и ее защищенности.

Таким образом, схема решения задачи синтеза ТС с учетом ПИБ опирается на теоретико-графовую модель и включает следующие процедуры:

1. Структурная оптимизация. На этом этапе осуществляется направленный перебор допустимых топологических структур СПД с учетом ПИБ. Этап выбора топологической структуры, соответствующий процедуре структурной оптимизации, может быть реализован методом случайного поиска, путем анализа типовых сетевых структур или путем выбора структуры сети на основании эвристических соображений.

2. Синтез базовой структуры с учетом ПИБ. Формирование базовых топологических структур можно осуществлять на основе двух подходов. Первый из них связан с заданием на известной узловой основе некоторой исходной допустимой (базовой) структуры и последующем ее преобразовании с целью достижения требуемых параметров. Второй заключается в последовательном введении на узловой основе всевозможных компонент связности — путей, деревьев и т.п. Первый подход представляется более предпочтительным, так как сужает область поиска на этапе структурной оптимизации, проще поддается формализации, позволяет судить

об оптимальности полученного решения, а также, в некоторых случаях исключает необходимость оценки промежуточных решений, полученных посредством преобразований базовой структуры.

3. Параметрическая оптимизация с учетом ПИБ. Представляет собой совокупность оптимизационных процедур — методов и алгоритмов, являющихся поисковыми процедурами, которые улучшают базовую структуру сети, последовательно изменяя ее участки.

Целью этапа параметрической оптимизации является достижение предельных значений параметров топологической структуры и безопасности в выбранном подклассе графов. Теоретико-графовая модель структуры СПД с учетом ПИБ несет минимум неструктурной информации, ее элементы обладает лишь свойствами существования и связности. Топологический характер объекта предполагает введение в теоретико-графовую модель ряда характеристик, определяющих количественную меру, и позволяет различать между собой варианты построения топологической структуры сети.

Оптимизация крупномасштабных распределенных телекоммуникационных сетей повлекла за собой необходимость отказа от громоздких матричных форм (матрицы инциденций, смежности и т.п.) и перехода к аналитическому описанию структурных параметров (диаметра, числа ребер, среднего расстояния, числа остовных деревьев и т.д.) и параметров информационной безопасности в виде функций числа вершин и узлов.

Таким образом, на основе анализа требований, тенденций развития сетей, средств и комплексов связи, условий их функционирования сформулированы общие задачи синтеза структуры СПД с учетом ПИБ как многокритериальной оптимизационной задачи в комбинаторном пространстве допустимых безопасных (защищенных) топологических структур. Обоснован выбор целевых функций, являющихся основными сетевыми характеристиками СПД и характеристиками информационной безопасности сетей такого класса. Решение данных задач базируется на декомпозиции общей задачи синтеза на ряд последовательных взаимоувязанных подзадач формирования безопасных топологической, потоковой и физических структур.

СПИСОК ЛИТЕРАТУРЫ

1. Рухман Е. Л., Ильин В. П., Смирнов М. И. Синтез топологических структур информационных сетей : учеб. пособие. Л.: ЛЭТИ, 1985. 79 с.
2. Шинкарев С. А., Паращук И. Б., Михайличенко А. В. Проактивный экспертный контроль структурной надежности сетей передачи данных и мобильных дата-центров для сбора и хранения электронных ресурсов в интересах инженерного образования // Совершенствование подготовки специалистов инженерных специальностей в контексте инновационного развития России. Проблемы и решения: материалы Международной заочной научно-практической и научно-методической конференции (15 ноября 2022 г.). СПб, Петергоф: ВИ (ЖДВ и ВОСО), 2023. С. 507-514.
3. Нехань Е. Н., Паращук И. Б., Скрябин Е. А. К вопросу функционального, организационного и структурного построения системы защиты информации при взаимодействии региональных корпоративных телекоммуникационных сетей с сетью общего пользования // Региональная информатика и информационная безопасность : сборник трудов. Вып. 4. СПб.: СПОИСУ.2017. С. 142-144.
4. Мизин И. А., Богатырев В. А., Кулешов А. П. Сети коммутации паке-тов / Под ред. В. С. Семенихина. М.: Радио и связь, 1986. 408 с.
5. Артамонов Г. Т., Тюрин В. Д. Топология сетей ЭВМ и многопроцессорных систем. М.: Радио и связь, 1991. 248 с.
6. Кристофидес Н. Теория графов. Алгоритмический подход / пер. с англ. М.: Мир, 1978. 432 с.
7. Татт У. Теория графов / пер. с англ. М.: Мир, 1988. 424 с.
8. Берж К. Теория графов и ее применения. / пер. с фр. ; под ред. И. А. Вайнштейна. М.: ИЛ, 1962. 319 с.
9. Kotenko I. V., Parashchuk I. B. Description of Information Security Events of Production and Technological Systems Using Fuzzy Graphs // 2022 International Russian Automation Conference (RusAutoCon), Sochi, Russia (4-10 Sept. 2022). IEEE Xplore Digital Library: Browse Conferences (2022). Vol. (Doc.) № 9896271. 2022. Pp. 45-50.

УДК 004.7

ПРИМЕНЕНИЕ МЕТОДА ЭКСТРЕМАЛЬНЫХ ПОРЯДКОВЫХ СТАТИСТИК ДЛЯ ОЦЕНКИ МАЛЫХ ЗНАЧЕНИЙ ВЕРОЯТНОСТЕЙ СЛУЧАЙНЫХ ВЕЛИЧИН

Янковский Никита Андреевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mail: yannik98@yandex.ru

Аннотация. Показано, что статистика экстремальных значений является эффективным средством решения задачи оценки малых значений вероятностей случайных величин. При соответствующем выборе структуры формулы экстраполяции, лежащей в основе экстремальных значений, можно значительно ускорить вычислительный эксперимент.

Ключевые слова: экстремальные порядковые статики; распределение с тяжелыми хвостами; распределение Вейбула; малые значения вероятностей случайных величин; время моделирования.

APPLICATION OF THE METHOD OF EXTREME ORDER STATISTICS FOR ESTIMATION OF SMALL PROBABILITIES OF RANDOM VARIABLES

Yankovskii Nikita
Saint Petersburg State University of Aerospace Instrumentation
67 Bolshaya Morskaya St, St. Petersburg, 190121 Russia
e-mail: yannik98@yandex.ru

Abstract. It is show that the statistics of extreme values is an effective tool for solving the problem of estimating small values of the probabilities of random variables. With an appropriate choice of the structure of the extrapolation formula underlying the extreme values, it is possible significantly speed up the computational experiment.

Keywords: Extreme Value Theory; distribution with heavy tails; Weibull distribution; small values of probabilities of random variables; simulation time.

Особенностью трафика современных инфокоммуникационных сетей с коммутацией пакетов является его масштабная инвариантность (фрактальность). Фрактальный трафик описывается долгосрочными зависимостями. Понятие пульсирующей структуры часто используется в этом контексте [1].

Адекватное описание фрактального трафика дают распределения вероятностей с тяжелыми хвостами [2]. Одним из таких примеров, используемых для описания пакетной структуры сетевого трафика, является распределение Вейбулла. Распределение Вейбулла широко используется в технике и представляет собой распределения с тяжелыми хвостами.

«Тяжелый хвост» означает, что в распределениях с тяжелыми хвостами значимые (большие) значения случайной величины более вероятны (чаще), чем те же значения, например, в экспоненциальном распределении.

Фрактальные свойства трафика оказывают существенное влияние на характеристики сети [3]. Решение многих задач теории и технологии информационных сетей требует оценки таких характеристик, как вероятность случайного превышения значения заданного значения. Это могут быть задачи, связанные с оценкой малых и очень малых вероятностей потери пакетов из-за переполнения буфера. Для таких задач решающей становится относительно небольшая часть значений случайных величин, задаваемых хвостом функции распределения.

Эффективным средством решения задач этого класса является статистика экстремальных значений. Это метод экстраполяции, основанный на знании асимптотического поведения распределения вероятностей [4]. «Хвост» вероятностного распределения значений случайной величины аппроксимируется зависимостью, параметры которой оцениваются по результатам прямого моделирования методом Монте-Карло [5, 6]. При правильном выборе структуры формулы экстраполяции можно значительно ускорить вычислительный эксперимент.

Целью доклада является представление решения задачи расчета вероятностно-временных характеристик сетевого узла с допустимой малой вероятностью потерь.

СПИСОК ЛИТЕРАТУРЫ

1. Шелухин О. И. Мультифракталы. Инфокоммуникационные приложения. М.: Горячая линия-Телеком, 2011. 576 с.
2. Татарникова Т. М. Анализ очередей и производительности узлов инфокоммуникационных сетей при обслуживании самоподобного трафика // Телекоммуникации. 2019. № 3. С. 6-11.
3. Татарникова Т. М., Вольский А. В. Оценка вероятностно-временных характеристик узлов с дифференциацией трафика // Информационно-управляющие системы. 2018. № 3 (94). С. 54-60. DOI: 10.15217/issn1684-8853.2018.3.54.
4. Королев В. Ю., Соколов И. А. Об условиях сходимости распределений статистики экстремальных порядков к распределению Вейбулла // Информатика и ее применение. 2014. № 3(8). С. 3-11.
5. Кутузов О. И., Татарникова Т. М. Из практики применения метода Монте-Карло // Заводская лаборатория. Диагностика материалов. 2017. Т. 83. № 3. С. 65-70.
6. Kutuzov O. I., Tatarnikova T. M. Model of a self-similar traffic generator and evaluation of buffer storage for classical and fractal queuing system // Proc. 1st Moscow Workshop on Electronic and Networking Technologies (MWENT 2018). 2018. P. 1–3. DOI: 10.1109/MWENT.2018.8337306.

УДК 004.8

ВЗАИМОСВЯЗЬ МАШИННОГО ЗРЕНИЯ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Яровой Роберт Владимирович, Паращук Игорь Борисович
Военная академия связи имени Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: Nadzar@yandex.ru, shchuk@rambler.ru

Аннотация. В данной статье исследуется взаимосвязь между машинным зрением и информационной безопасностью. Рассматривается значимость информационной безопасности в современном информационном обществе и роль, которую играет машинное зрение в обеспечении безопасности данных. Анализируются различные способы применения машинного зрения в системах безопасности, а также обсуждаются потенциальные угрозы и методы обеспечения безопасности в контексте машинного зрения. Представлены перспективы развития в области безопасности машинного зрения, включая прогнозирование угроз, развитие стандартов безопасности и этические аспекты.

Ключевые слова: машинное зрение, информационная безопасность, визуальный анализ, угрозы, защита, аутентификация, обнаружение аномалий.

THE INTERCONNECTION OF MACHINE VISION AND INFORMATION SECURITY

Yarovoy Robert, Parashchuk Igor
Military Academy of Communications Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av., St. Petersburg, 194064, Russia
e-mails: Nadzar@yandex.ru, shchuk@rambler.ru

Abstract. This article explores the relationship between machine vision and information security. The importance of information security in the modern information society and the role played by machine vision in ensuring data security are considered. Various ways of using machine vision in security systems are analyzed and potential threats and methods for ensuring security in the context of machine vision are discussed. Prospects for development in the field of machine vision security are presented, including threat prediction, development of security standards and ethical aspects.

Keywords: machine vision, information security, visual analysis, threats, protection, authentication, anomaly detection.

В современном информационном обществе, где данные играют ключевую роль, обеспечение информационной безопасности становится все более важным. Защита конфиденциальности, целостности и доступности информации становится приоритетом для организаций и индивидуальных пользователей. В этом контексте машинное зрение, являющееся разделом искусственного интеллекта, предоставляет мощные возможности анализа и обработки визуальной информации, что приводит к появлению новых решений в области информационной безопасности. С помощью алгоритмов искусственного интеллекта, машинное зрение может выполнять такие задачи, как распознавание объектов, классификация изображений, обнаружение лиц, анализ поведения и многое другое [1].

Однако, вместе с возможностями машинного зрения возникают новые угрозы информационной безопасности. Визуальные данные, которые являются основой машинного зрения, могут быть подвержены атакам и злоупотреблениям. Например, злоумышленники могут попытаться подменить или изменить визуальные данные, чтобы обмануть системы распознавания или получить несанкционированный доступ к информации. Кроме того, системы машинного зрения могут стать целью атак, направленных на компрометацию их функциональности или получение конфиденциальной информации, которая используется в процессе обработки. Для обеспечения безопасности систем машинного зрения необходимы эффективные меры защиты. Криптографические методы, методы аутентификации и авторизации, а также методы обнаружения аномалий играют важную роль в предотвращении и обнаружении атак на системы машинного зрения. Безопасность машинного зрения также требует разработки и применения соответствующих стандартов и регуляций, чтобы обеспечить надежность и доверие к этим системам [2].

Машинное зрение играет важную роль в анализе визуальных данных с целью выявления потенциальных угроз. Например, системы машинного зрения могут использоваться для мониторинга видео потоков с камер наблюдения и автоматического обнаружения подозрительных действий или вторжений. Алгоритмы машинного зрения позволяют автоматически анализировать и классифицировать объекты и события на видеозаписях, что облегчает задачу обнаружения возможных угроз. Системы машинного зрения также могут быть применены для определения и распознавания объектов, что имеет прямое отношение к информационной безопасности. Например, системы распознавания лиц могут использоваться для контроля доступа в организациях и обнаружения несанкционированного проникновения.

Еще одним важным применением машинного зрения в информационной безопасности являются системы видеонаблюдения и анализа поведения. Такие системы могут непрерывно обрабатывать видеопотоки и автоматически обнаруживать аномальное поведение. Например, алгоритмы машинного зрения могут определять оставленные без присмотра объекты или необычное движение, что может свидетельствовать о потенциальной угрозе или возникновении проблемы в системе безопасности.

Применение машинного зрения в информационной безопасности позволяет автоматизировать процессы обнаружения и анализа, что снижает нагрузку на операторов и повышает эффективность систем безопасности. Однако, необходимо учитывать потенциальные угрозы и риски, связанные с такими системами. Системы машинного зрения могут быть подвержены различным атакам, направленным на компрометацию их функциональности или получение неправомерного доступа к важным данным [3]. Некоторые распространенные атаки включают атаки отказа в обслуживании, при которых злоумышленник стремится насытить ресурсы системы машинного зрения, чтобы она перестала функционировать или работала со сниженной производительностью. Также могут быть проведены атаки переполнения буфера, внедрение вредоносного кода или использование уязвимостей в программном обеспечении системы машинного зрения для получения контроля над ней. Существует угроза модификация или подмены визуальных данных, которые используются системами машинного зрения [4]. Злоумышленники могут изменить содержимое изображений или видео, чтобы обмануть системы распознавания или исказить результаты анализа. Например, это может привести к неправильному распознаванию объектов или обходу систем контроля доступа на основе распознавания лиц. Эта угроза становится особенно актуальной в контексте систем видеонаблюдения и анализа поведения, где точность и надежность результатов анализа играют важную роль.

Системы распознавания лиц и идентификации могут также подвергаться специальным атакам, направленным на обход их защиты. Злоумышленники могут использовать различные методы, такие как подделка или маскировка лица, для обмана систем распознавания. Это может привести к несанкционированному доступу или подделке личности. Поэтому необходимо постоянно совершенствовать алгоритмы и методы, используемые в системах распознавания лиц, чтобы они были более устойчивыми к таким атакам. Понимание этих угроз информационной безопасности в машинном зрении является важным для разработки соответствующих мер защиты. Криптографические методы являются одним из основных инструментов для защиты данных в системах машинного зрения [5]. Шифрование данных может применяться для обеспечения конфиденциальности при

передаче или хранении визуальной информации. Криптографические протоколы также могут быть использованы для аутентификации и целостности данных, чтобы предотвратить их модификацию или подмену. Применение криптографических методов требует разработки безопасных ключей и протоколов, а также эффективных алгоритмов шифрования, учитывающих специфику обработки визуальных данных.

Аутентификация и авторизация играют важную роль в обеспечении безопасности систем машинного зрения. Для предотвращения несанкционированного доступа к системам машинного зрения необходимо использовать надежные методы аутентификации, такие как системы распознавания лиц, сканирование отпечатков пальцев или многофакторную аутентификацию. Для защиты систем машинного зрения от атак необходимо разрабатывать и применять методы обнаружения аномалий и защиты от атак. Методы обнаружения аномалий позволяют идентифицировать необычные или подозрительные паттерны в данных машинного зрения, что может указывать на наличие атаки или аномального поведения. Это включает мониторинг активности системы, анализ аномальных показателей и создание профилей обычного поведения для сравнения. Кроме того, разработка и применение защитных механизмов, таких как межсетевые экраны, системы обнаружения вторжений и защита от вредоносных программ, играют важную роль в обеспечении безопасности систем машинного зрения. Методы обеспечения безопасности машинного зрения являются активной областью исследований, и постоянно развиваются новые подходы для более эффективной защиты

Развитие машинного зрения и его применение в информационной безопасности поднимает важные этические вопросы. Например, использование систем распознавания лиц может повлечь за собой нарушение приватности и индивидуальных прав. Поэтому важно разрабатывать этические принципы и нормы, которые помогут сбалансировать потенциальные пользу и возможные риски от применения машинного зрения в информационной безопасности. Все эти аспекты будут продолжать развиваться и требовать внимания и совместных усилий со стороны исследователей, разработчиков, регуляторных органов и общества в целом. Обеспечение безопасности машинного зрения должно быть в центре внимания, чтобы гарантировать прогресс и применение этой технологии в безопасном и этически обоснованном контексте.

Таким образом, рассмотрены взаимосвязь между машинным зрением и информационной безопасностью. Машинное зрение предоставляет мощные возможности анализа и обработки визуальной информации, но при этом сталкивается с различными угрозами информационной безопасности. Обеспечение безопасности машинного зрения требует применения различных методов, включая криптографические методы, аутентификацию и авторизацию, а также методы обнаружения аномалий и защиты от атак. Дальнейшее развитие машинного зрения и информационной безопасности требует прогнозирования угроз, разработки стандартов и регулирования, а также учета этических аспектов.

СПИСОК ЛИТЕРАТУРЫ

1. Методы обработки и распознавания изображений лиц в задачах биометрии / Г. А. Кухарев [и др.]. М.: Политехника, 2013. 416 с.
2. Шкодырев В. П., Ягафаров К. И., Баштовенко В. А., Ильина Е. Э. Обзор методов обнаружения аномалий в потоках данных // Proc. of the Second Conference on Software Engineering and Information Management. Санкт-Петербург, 2017. Vol. 1864. С. 7-9.
3. Круглов В. В., Борисов В. В. Искусственные нейронные сети. Теория и практика. М.: Горячая линия-Телеком, 2001. 234 с.
4. Галушкина А. И. Теория нейронных сетей. М.: ИПРЖР, 2000. 233 с.
5. Гладких А. А., Дементьев В. Е., Чилихин Н. Ю. Основы современных криптографических систем и перспективы их развития : учеб. пособие. Ульяновск: УлГТУ, 2020. 214 с.

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 004.056

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТИ КОМПАНИЙ ПО СОЗДАНИЮ КОМПЬЮТЕРНЫХ ИГР

Аминов Хакимджон Иномджонович, Урванцев Роман Алексеевич
Санкт-Петербургский государственный экономический университет
наб. канала Грибоедова, 30-32, лит. А., Санкт-Петербург, 191023, Россия
e-mails: h_aminov@unecon.ru, roman@urwantsev.ru

Аннотация. В докладе рассматриваются основные угрозы и подходы к обеспечению информационной безопасности в деятельности компаний по разработке многопользовательских компьютерных игр.

Ключевые слова: угрозы, информационная безопасность, подходы, компания, компьютерные игры.

APPROACHES TO ENSURING INFORMATION SECURITY IN THE ACTIVITIES OF THE GAME DEVELOPMENT COMPANIES

Aminov Khakimdzhon, Urvantsev Roman
Saint Petersburg State University of Economics
30-32 Griboedov canal emb., St. Petersburg, 191023, Russia
e-mails: h_aminov@unecon.ru, roman@urwantsev.ru

Abstract. The report deals with the main threats and approaches to ensuring information security in the activities of multiplayer game development companies.

Keywords: threats, information security, approaches, company, computer games.

В последние годы все больше растет интерес пользователей к компьютерным играм [1]. Однако с увеличением количества людей, работающих из дома и повышением интереса к компьютерным играм, также выросло количество киберпреступлений [2], в том числе и в игровой среде. Это подтолкнуло компании-разработчиков игр принять меры по обеспечению информационной безопасности, внедрению и поддержанию защитных механизмов данных своих игроков, и обучению основам информационной безопасности в сети среди пользователей игровых сервисов.

Основные проблемы информационной безопасности в деятельности компаний по разработке компьютерных игр связаны с умышленными угрозами, так как они часто становятся причиной преступлений и нарушений законодательства.

Большинство нарушений в сфере информационной безопасности происходят из-за внутренних угроз, таких как утечка данных, кража коммерческой тайны и личных данных клиентов, а также повреждение компьютерных ресурсов [3].

Преступления, которые причиняют вред интеллектуальной и коммерческой собственности организации, а также кража персональных данных пользователей, связаны с «инсайдами». Существуют две категории инсайдерских действий: злонамеренные и непреднамеренные. Злонамеренные инсайдеры могут быть сотрудниками, которые имеют злобу на компанию, стремятся подзаработать на ней или были завербованы для выполнения преступных действий внутри организации. Самым опасным типом злоумышленников являются внедрённые и завербованные инсайдеры, которые могут являться частью организованных преступных групп или групп по коммерческому шпионажу.

Помимо внутренних угроз информационной безопасности самой компании, также остро стоит вопрос о внутриигровых угрозах для пользователя. Такими угрозами могут стать мошеннические действия с виртуальным имуществом пользователя и его вовлечение в использовании «черного рынка», под которыми следует понимать услуги по обмену внутриигровых ценностей на настоящие деньги. Однако это далеко не все угрозы, которые могут подстерегать пользователей игровых сервисов. Основными угрозами считаются следующие: взлом аккаунтов; кража информации пользователей; фишинг; распространение вирусов через программы; мошенничество; DDoS-атаки для отключения игровых серверов [4].

Рассмотрим основные подходы к борьбе с подобными угрозами.

Для борьбы с кражей информации пользователей и фишингом существует несколько способов. Первый и, пожалуй, самый важный способ — это повышение осведомленности пользователей о том, как работает фишинг и какие могут быть признаки мошенничества. Компании должны обучать своих сотрудников и давать

рекомендации пользователям, как распознавать подозрительные электронные письма и сообщения, а также не раскрывать личную информацию, не переходить по подозрительным ссылкам и не скачивать подозрительные вложения. Также следует использовать и регулярно обновлять антивирусное программное обеспечение, чтобы устранять уязвимости, которые могут быть использованы злоумышленниками для проведения атак фишинга.

Для борьбы со взломом аккаунтов существуют несколько способов. Самым важным является использование сложных и надежных паролей, которые состоят из букв разного регистра, цифр и специальных символов, а также их регулярная смена. Кроме этого, можно использовать механизмы защиты от взлома аккаунтов, такие как установка временной задержки между попытками ввода пароля, использование «капчи», блокировка аккаунта после нескольких неудачных попыток ввода пароля и т.д. Среди дополнительных методов защиты можно отметить двухфакторную аутентификацию. Для этого могут быть использованы, например, приложения Яндекс.Ключ и Google Authenticator.

Среди наиболее распространённых атак можно выделить «отказ в обслуживании» (Distributed Denial of Service), который используется для парализации работы веб-сервера, что потребует от компании-разработчика тратить средства и силы на отражение этой атаки, теряя выгоду.

Наилучшей защитой от подобных атак является ряд действий, которые смогут помочь в отражении атак [5]:

– выбор надежного хостинг-провайдера, который предоставляет надежную защиту от угроз и доступ к статистике и имеет круглосуточную техподдержку;

– запрет доступа для третьих лиц к сетевой инфраструктуре, а для собственных сотрудников доступ должен быть строго регламентирован;

– использование Firewall, VPN, CDN. Необходимо фильтровать трафик и обеспечить его безопасность, также использовать межсетевые экраны либо списки ACL;

– предотвращение спама через использование captcha;

– создание резервных ресурсов — необходимо убедиться, что хостинг-провайдер предоставляет избыточную пропускную способность подключения.

Игровые сервисы представляются легкой добычей для злоумышленников, которые применяют методы социальной инженерии. Они могут легко получить личную информацию, попросив игроков предоставить ее, войдя в их доверие, став друзьями, проводя много времени вместе в виртуальном мире. В этом случае для уточнения данных в первую очередь следует обратиться к администраторам игровых сервисов.

Для обеспечения информационной безопасности и сведения подобных рисков к минимуму имеются различные подходы в зависимости от рода этих угроз.

Обеспечение информационной безопасности в случае внутренних угроз требует комплексного подхода. Он выражается в следующих действиях: обучении сотрудников; разграничении доступа; мониторинге действий сотрудников; соблюдении политики безопасности; аудите безопасности; использовании систем контроля доступа; контроле за сетевым трафиком.

Обеспечение внутриигровой безопасности пользователя в свою очередь реализуется: введением справедливых, но строгих правил в отношении внутриигровых нарушений; введением жестких правил и наказаний за нарушение лицензионного соглашения; выпуском обучающих материалов для пользователей об обеспечении безопасности учетной записи; выявлением и противодействием возможным мошенническим действиям в самой игре.

При построении защищенной системы игрового сервиса следует также использовать «Методический документ. Методика оценки угроз безопасности информации», утвержденный ФСТЭК России 5 февраля 2021 года [6].

Подводя итоги, следует отметить, что информационная безопасность зависит как от действий компаний-разработчиков, так и пользователей. Компании должны обеспечить конфиденциальность данных пользователей и своевременно реагировать на возможные угрозы информационной безопасности, разрабатывать и реализовывать грамотную политику безопасности серверов и использовать необходимые программное и аппаратное обеспечение. Пользователь в свою очередь может предпринять шаги для защиты своего аккаунта, включая настройку безопасности, такую как двухфакторная аутентификация, сложный и уникальный пароль, а также проверенный адрес электронной почты. Это может существенно уменьшить риск атак на аккаунт. Пользователи должны быть бдительны и внимательны, особенно при работе с незнакомыми сайтами и приложениями, а также при получении подозрительных сообщений или электронной почты. Только совместные усилия компаний и пользователей могут помочь снизить количество инцидентов и обеспечить информационную безопасность.

СПИСОК ЛИТЕРАТУРЫ

1. Попов И. Оцифрованные: как пандемия повлияла на игровую индустрию // Сетевое издание «forbes.ru». URL: https://www.forbes.ru/tehnologii/420471-ocifrovannye-kak-pandemiya-povliyala-na-igrovuyu-industriyu (дата обращения: 30.06.2023).
2. Число киберпреступлений в России // Интернет-портал и аналитическое агентство TAdviser. URL: https://www.tadviser.ru/index.php/Статья:Число__киберпреступлений_в_России (дата обращения: 30.06.2023).
3. Аминов Х. И., Дремезова А. А. Опасности цифровой среды для бизнеса и общества // Цифровые опасности информационного общества. Сборник статей / под редакцией И. Л. Коршунова. СПб : Изд-во СПбГЭУ, 2023. С. 20-29.
4. Онлайн-игры: 10 основных рисков и как их избежать // АО «Лаборатория Касперского». URL: https://www.kaspersky.ru/resource-center/threats/top-10-online-gaming-risks (дата обращения: 30.06.2023).
5. Антипов О. Как защититься от DDoS-атак: ТОП-10 способов // ООО «ДДОС-ГВАРД». URL: https://ddos-guard.net/ru/blog/sposoby-zashity-ot-ddos-atak (дата обращения: 30.06.2023).
6. Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021) // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_378330/ (дата обращения: 30.06.2023).

УДК 004

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ СИСТЕМ ВОДОСНАБЖЕНИЯ И ВОДООТВЕДЕНИЯ

Аникин Юрий Викторович, Шилков Владимир Ильич, Ушакова Людмила Ивановна
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина
Мира ул., 19, Екатеринбург, 620002, Россия
e-mails: anikin-urfu@yandex.ru, shilkov-urfu@yandex.ru, light_uli@mail.ru

Аннотация. Обсуждаются вопросы информационной и экономической безопасности систем водоснабжения и водоотведения. Приведены сведения, подтверждающие актуальность и необходимость применения защиты систем водоснабжения и водоотведения от негативного внешнего воздействия. Приведены рекомендации по повышению уровня их кибербезопасности и организации подготовки специалистов для отрасли.

Ключевые слова: информационно-коммуникационные технологии; системы водоснабжения и водоотведения; информационные технологии; террористические атаки, кибербезопасность.

RUSSIAN AND FOREIGN EXPERIENCE OF DIGITALIZATION WATER SUPPLY AND SANITATION SYSTEMS

Anikin Yuri, Shilkov Vladimir, Ushakova Ludmila
Ural Federal University named after the First President of Russia B. N. Yeltsin
19 Mira St, Yekaterinburg, 620002, Russia
e-mails: anikin-urfu@yandex.ru, shilkov-urfu@yandex.ru, light_uli@mail.ru

Abstract. The issues of information and economic security of water supply and sanitation systems are discussed. The information confirming the relevance and necessity of the use of protection of water supply and sanitation systems from negative external influences is given. Recommendations are given for improving their cybersecurity level and organizing training of specialists for the industry.

Keywords: information and communication technologies; water supply and sanitation systems; information technologies; terrorist attack, cybersecurity.

Системы водоснабжения и водоотведения играют значительную роль в жизнедеятельности общества, которую невозможно недооценивать. Вода нужна не только для хозяйственно-питьевых и бытовых нужд, но в большом и даже значительно большем количестве нужна в промышленности, в сельском хозяйстве и для других целей. В современном мире деятельность систем водоснабжения и водоотведения невозможно представить без применения информационно-коммуникационных технологий в производственных, технологических и административных процессах.

Применение информационно-коммуникационных технологий позволяет значительно повысить эффективность и качество управления системами водоснабжения и водоотведения, применить современное технологическое оборудование, основанное на данных технологиях. С другой стороны, воздействие на работу таких систем, связанное с хакерским вмешательством в системы управления (SCADA и другие), может привести к нежелательным последствиям (экономическим, материальным).

Способность систем водоснабжения и водоотведения к надежному функционированию относится к одной из важных задач городских инфраструктур. Нарушение деятельности этих систем может оказать негативное влияние на обеспечение населения безопасной питьевой водой, очистку сточных вод до нормативных требований, приведет к загрязнению окружающей среды, вызовет сбои в работе различных предприятий. В этом смысле объекты систем водоснабжения и водоотведения, в частности их информационно-коммуникационных технологий, напрямую связаны с региональной безопасностью.

Вопросы информационной безопасности систем водоснабжения и водоотведения являются актуальными для любой страны. Приведем ряд примеров, показывающих злоумышленные действия, направленные на объекты таких систем и описывающие последствия этих действий. Так житель Канзаса в марте 2019 года умышленно незаконно получил доступ к защищенной системе водоснабжения в штате Канзас и пытался повлиять на процедуры очистки и дезинфекции воды, что привело к остановке технологических процессов объекта. Как отмечено в [1], «незаконно вмешиваясь в общественную систему питьевого водоснабжения, обвиняемый угрожал безопасности и здоровью целого сообщества». В другой работе [2], говорится о нескольких случаях в период с марта по август 2021 года, когда злоумышленники в различных городах США проявили несколько вредоносных кибератаки, нацеленных на сети, системы и устройства сектора информационных технологий и операционных технологий объектов систем водоснабжения и водоотведения. Сообщается, что упомянутые киберинциденты указывают на то, что злоумышленники хорошо разбираются в операционных технологиях, функционирующих в секторе водоснабжения, и осознают ущерб, который они могут нанести, начав кибератаки на объекты водоснабжения. В работе [3] дается исторический обзор безопасности критической инфраструктуры водных ресурсов и их зависимостей в связи с терроризмом или неблагоприятным вмешательством человека.

В январе 2022 года администрация президента США объявила об Инициативе по кибербезопасности промышленных систем управления в секторе водоснабжения и водоотведения (Water Sector Action). Этот план

представляет собой совместную работу федерального правительства и сообщества, занимающегося критически важной инфраструктурой, по содействию внедрению технологий и систем, обеспечивающих видимость киберугроз, индикаторов, обнаружения и предупреждений. Показано [4], что хакеры-злоумышленники долгое время использовали недостатки, обнаруженные в компонентах систем водоснабжения и водоотведения, для атак на объекты этих систем.

При решении задач, связанных с созданием эффективных и безопасных информационных систем комплексов водоснабжения и водоотведения, необходимо учитывать тот факт, что такие комплексы представляют собой сложные энергоемкие системы с развитой организационной структурой и большим количеством разнородных технологических и сопутствующих процессов. Необходимость измерения и оценки количественных и качественных характеристик природных поверхностных и подземных водных ресурсов требует применения автоматизированных информационных систем с большим количеством разнообразных датчиков, возможностью передавать собранные данные на значительные расстояния и обрабатывать их. На состояние информационно-экономической безопасности систем водоснабжения и водоотведения в значительной степени может влиять целый ряд факторов и специфических особенностей не только отдельных производственных компонентов, но и полных организационно-технологических процессов циклов водоподготовки.

Актуальность проблемы и необходимость создания эффективной защиты критической информационной инфраструктуры обусловили принятие соответствующих решений. Так, например, для повышения уровня безопасности критической информационной инфраструктуры: с 1 января 2025 года организациям и предприятиям в Российской Федерации запрещается использовать средства защиты информации, произведённые в недружественных к странах; определены требования к аппаратно-программному обеспечению; актуализируются профессиональные стандарты и квалификационные требования по подготовке специалистов в IT-отрасли; вносятся изменения в нормативную базу по защите критической информационной инфраструктуры.

Как показывает проведенное исследование, для достижения необходимого уровня информационно-экономической безопасности целесообразно применение методов системного подхода с целью анализа экономических, организационных и технологических факторов работы систем водоснабжения и водоотведения. К сожалению, традиционным экономическим препятствием, в значительной степени определяющим уровень информационно-экономической безопасности систем водоснабжения и водоотведения, остается хроническая недоинвестированность отрасли. Отсутствие необходимых экономических средств приводит не только к прогрессирующей усталости основного оборудования, участков сетей, низкому уровню энергосбережения и моральному устареванию технологий, но и делает невозможным реализацию инновационных стратегий развития в области внедрения безопасных информационных и автоматизированных комплексов.

Уязвимости в информационной безопасности систем водоснабжения и водоотведения могут быть также связаны как с организационными, технологическими, психологическими факторами и с характеристиками информационных технологий, инструментов, программно-аппаратных комплексов, используемых для целей управления системами.

Анализ проблемных моментов, связанных с информатизацией процессов водоподготовки и очистки сточных вод показывает, что к основным проблемам, связанным с внедрением информационных систем в различные комплексы водоснабжения и водоотведения, следует отнести: отсутствие комплексных ИТ-решений и стандартов цифровой трансформации, ориентированных на отрасль, а также низкий уровень цифровой грамотности и неготовность большинства сотрудников предприятий применять информационные технологии для целей управления. Для повышения уровня информационной безопасности систем целесообразно проведение ряда первоочередных мероприятий, к которым можно отнести мероприятия по организации постоянного мониторинга систем контроля объектов критической инфраструктуры и создание центров обработки информации для анализа уязвимостей и инцидентов, ранее уже имевших место в информационных системах защиты объектов водоснабжения и водоотведения. Система для осуществления мониторинга должна охватывать все подключаемые к внешним интернет сетям уязвимые и чувствительные к кибератакам элементы, через которые хакеры могут получить доступ к информации, необходимой для определения направлений атак с последующим получением контроля над критически значимыми элементами систем управления объектами водоснабжения и водоотведения.

СПИСОК ЛИТЕРАТУРЫ

1. Indictment: Kansas man indicted for tampering with a public water system. Press release. March 31, 2021. URL: https://www.justice.gov/usao-ks/pr/indictment-kansas-man-indicted-tampering-public-water-system (дата обращения: 20.06.2023).
2. Ongoing cyber threats to U. S. water and wastewater systems. Cybersecurity advisory. October 25, 2021. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a (дата обращения: 20.06.2023).
3. Birkett D. M. Water Critical Infrastructure Security and Its Dependencies // Journal of Terrorism Research, 2017. № 8(2). Pp. 1–21. DOI: http://doi.org/10.15664/jtr.1289 [Электронный ресурс]. URL: https://cvir.st-andrews.ac.uk/articles/10.15664/jtr.1289/ (дата обращения: 20.06.2023).
4. Fact Sheet: Biden-Harris Administration Expands Public-Private Cybersecurity Partnership to Water Sector. Statements and releases. January 27, 2022. [Электронный ресурс]. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/27/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-water-sector/ (дата обращения: 20.06.2023).

УДК 004.9

УЛУЧШЕНИЕ МЕТОДОВ ЗАЩИТЫ В СИСТЕМАХ РАДИОЧАСТОТНОЙ АВТОРИЗАЦИИ

Емельянов Александр Александрович, Мелихова Валентина Евгеньевна
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, Россия, 191023
e-mail: S1_Alex2000@mail.ru

Аннотация. Рассмотрены общие концепции систем авторизации на базе радиочастотных подходов с использованием аппаратных методов. Указаны потенциальные уязвимости имеющихся решений. Предложена схема улучшения безопасности систем РЧ-авторизации.

Ключевые слова: авторизация, безопасность, доступ.

IMPROVING SECURITY METHODS IN RADIO FREQUENCY AUTHORIZATION SYSTEMS

Emelyanov Alexandr, Melikhova Valentina
St. Petersburg State University of Economics
21 Sadovaya st., St. Petersburg, Russia, 191023
e-mail: S1_Alex2000@mail.ru

Abstract. The general concepts of authorization systems based on radio frequency approaches with the use of hardware methods are considered. Potential vulnerabilities of existing solutions are indicated. A scheme for improving the security of RF authorization systems is proposed.

Keywords: authorization, security, access.

Одним из важных аспектов информационно-экономической безопасности на предприятиях является контрольно-пропускная система, с помощью которой сотрудники получают доступ во внутренний периметр помещения. Значимость этого аспекта весьма велика: обычно меры защиты внутри предприятия значительно слабее, нежели при внешнем доступе. Злоумышленник, который получил возможность взаимодействовать с аппаратно-программными комплексами напрямую, способен с минимальными усилиями похитить либо исказить информацию, влияющую на экономическую эффективность работы предприятия. Внесение изменений в базы данных клиентов и поставщиков; дублирование информации с последующим созданием конкурирующей структуры; хищение персональных данных сотрудников; несанкционированный перевод финансовых активов предприятия на сторонние счета — это малая часть деструктивных действий, которые становятся возможными в случае проникновения и доступа ко внутренним IT-ресурсам предприятия [1].

Для снижения вероятности подобных событий применяются системы биометрической и аппаратной аутентификации. На текущий момент стационарные АПК для точной идентификации личности по индивидуальным биологическим характеристикам являются вторичными средствами из-за их дороговизны и ненадёжности срабатывания. Кроме того, велика вероятность имитации с использованием баз отпечатков пальцев, лицевых моделей и доступных решений для их воспроизводства — например, 3Д-принтеров. Вследствие этого для большинства предприятий основным средством авторизации является применение ключ-карт и RFID-меток, часто совмещаемых с вышеописанными системами биометрического распознавания.

При использовании ключ-карт и брелоков, работающих в радиодиапазоне, реализуется две возможных схемы. В первом случае ЭМ-генератор АПК формирует поле, создающее в катушке портативного приёмника наведённую ЭДС, с помощью которого активируется модуль, создающий «отклик», в свою очередь, воспринимаемый стационарным устройством, которое проверяет — соответствуют ли характеристики сигнала заранее предустановленным паттернам. Во втором случае сам мобильный модуль содержит в себе источник питания, являясь активным источником радиосигнала, который принимается стационарным блоком и проверяется на соответствие. В качестве основных подходов криптозащиты применяется, опять же, два варианта. Первый подразумевает фиксированную кодовую последовательность (большинство ключ-карт, «таблеток» домофонов и аналогичных устройств). Второй — использование динамического роллинг-кода, когда каждый сеанс авторизации является уникальным с точки зрения характеристик генерируемого радиосигнала.

У каждого из рассмотренных выше видов устройств имеется фундаментальная уязвимость, позволяющая с минимальными затратами имитировать оригинальный ключ-брелок. Использование устройств класса «флиппер зеро» в суб-гигагерцовом диапазоне позволяет не просто перехватить и проанализировать raw-код, но и сгенерировать его при взаимодействии с устройством проверки. Таким способом можно обходить системы авторизации домофонов, автомобилей, сканирующие АПК, установленные на КПП и т.д. Единственный аспект, которым будет отличаться стационарный код от роллинг-версии — это количество раз авторизации с одной версией кода, которое будет считать валидными система контроля [2].

Данная уязвимость может быть сведена к минимуму гибридной системой вопросно-ответных согласований по аналогии с теми, что реализуются в протоколе https на основе tls, а также в рамках стандарта 802.11. Предлагаемый алгоритм сводится к следующим шагам. Мобильный брелок генерирует РЧ-запрос к стационарному устройству, предлагая согласовать взаимодействие и осуществить аутентификацию. Стационарный АПК принимает запрос и, в свою очередь, запрашивает сертификат у брелока, который может быть представлен в виде генерируемой псевдослучайной последовательности с плавающим законом

вероятностного распределения значений. В случае, если полученный от брелока сертификат соответствует некоторым заранее предустановленным правилам (с учётом малых вычислительных возможностей конечных устройств и потенциальных искажений радиочастотной передачи), стационарный АПК активирует алгоритм псевдослучайной перестройки рабочей частоты в соответствии с присланными брелоком и проверенными на предыдущем шаге значениями. Дальнейший радиообмен осуществляется со скачкообразной сменой частоты и может включать в себя различные криптоалгоритмы — как симметричные, так и несимметричные [3].

Предлагаемый вариант позволит существенно осложнить перехват и генерацию фальшивого сигнала имитационными устройствами. Это позволит повысить надёжность устройств для авторизации сотрудников, снизить вероятность проникновения на территорию предприятий нелегальных личностей, свести к минимуму потенциальные ситуации НСД. В свою очередь, решение описанных задач снизит фактор информационно-экономических рисков в работе предприятий.

СПИСОК ЛИТЕРАТУРЫ

1. Методологические основания технологических инноваций цифровой экономики / Аминов Х.И. [и др.]. СПб : СПбГЭУ, 2023. 203 с.
2. Демидов А. В., Емельянов А. А. Анализ уязвимостей и разработка требований к безопасности в современной IT-инфраструктуре : статья в сборнике статей. / под ред. И. Л. Коршунова. СПб : СПбГЭУ, 2023. С. 42–48.
3. Пуха Г. П., Пищальников С. М., Емельянов А. А. Методика оценивания помехоустойчивости радиолиний обмена данными с временным разделением каналов // Известия высших учебных заведений. Приборостроение, 2021. № 11. Т. 64. С. 887–895.

УДК 004.738

ПРИОРИТЕТНАЯ МОДЕЛЬ ПРОЦЕССА ОБМЕНА ДАННЫМИ В ЦИФРОВОМ ДВОЙНИКЕ

Краснова Анна Сергеевна[1], Колбанёв Михаил Олегович[2]
[1] Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия
[2]Санкт-Петербургский государственный экономический университет
наб. канала Грибоедова, 30-32, Санкт-Петербург, 191023, Россия
e-mails: shochina96@mail.ru, mokolbanev@mail.ru

Аннотация. Рассмотрена приоритетная модель процесса обмена данными на примере цифровых двойников при использовании различных законов.

Ключевые слова: цифровой двойник, модель, приоритет, обмен данными.

PRIORITY MODEL OF THE DATA EXCHANGE PROCESS IN A DIGITAL DOUBLE

Krasnova Anna [1], Kolbanev Mikhail [2]
[1]Nizhny Novgorod State University of Engineering and Economics
22a Oktyabrskaya St., Knyaginino, 606340, Russia
[2]St. Petersburg State University of Economics
30-32 nab. Griboyedov Canal, St. Petersburg, 191023, Russia
e-mails: shochina96@mail.ru, mokolbanev@mail.ru

Abstract. The priority model of the data exchange process is considered on the example of digital twins using various laws.

Keywords: digital twin, model, priority, data exchange.

Человечество вступает в новую эпоху, эпоху интеллектуальных технологий. Все то, что нас окружает стремительно изменяется и эволюционирует. Мы вступаем в век, где интеллектуальные системы способны выполнять функции оптимизации, принятия решения, автоматического анализа и многих других функций взаимодействуя при этом с реальным миром в режиме реального времени [1].

На стыке нескольких цифровых технологий появляются новые решения. Ярким примером является концепция цифровых двойников (ЦД, Digital Twins). Цифровые двойники призваны облегчать средства контроля, понимания и оптимизации функций всех физических активов, обеспечивая беспрепятственную передачу данных между физическим и виртуальным миром [2].

Согласно определению Центра компетенций НТИ СПбПУ, «Новые производственные технологии», цифровой двойник — это, прежде всего, технология, процесс проектирования, в основе которого лежит разработка и применение семейства сложных мультидисциплинарных математических моделей, описываемых 3D нестационарными нелинейными дифференциальными уравнениями в частных производных [3].

Анализируя существующие понятия и области исследования цифровых двойников, будем считать, что цифровой двойник — это созданная в киберпространстве цифровая (информационная, виртуальная) модель (копия, описание, профиль) некоторых физических сущностей (объектов, процессов), взаимодействующих в режиме реального времени, по отношению к этой модели физическая сущность представляет собой оригинал. Цифровой двойник характеризуется двунаправленным потоком данных между цифровой и физической сущностью. Взаимодействие цифрового двойника и его физического объекта должно быть непрерывным. Данные передаются в режиме реального времени, и соответственно для производительности систем, необходимо учитывать способность безопасно и эффективно собирать, передавать и анализировать потоки данных между объектами физической системы и кибер-системой. Качество процесса предоставления информационной услуги

оценивается вероятностью своевременной обработки запроса пользователя, под которой понимается вероятность того, что ответ на запрос будет получен за допустимое время [4].

Будем считать, что каждый датчик, а их может быть n — количество, формируют экспоненциальный поток данных — λ, для каждого потока данных, имеющих относительный приоритет, известно допустимое время с момента измерения параметра, до момента передачи их в цифровой двойник и его изменение. Допустимое время при передаче данных, имеющих приоритет, задано распределением Эрланга. При расчете времени $t_h(s)$ процесса предоставления услуги для каждого приоритета, будем использовать преобразование Лапласа-Стилтьеса для расчета времени ожидания начала обработки, времени обработки в сервере и времени доставки к серверу через среду множественного доступа. В зависимости от определенного закона распределения, время обработки в сервере по преобразованию Лапласа-Стилтьеса будет иметь свой вид, тем самым путем соответствующего выбора значений параметров, функцией допустимого времени можно достаточно точно аппроксимировать любую реальную функцию реализации допустимого времени предоставления услуги.

СПИСОК ЛИТЕРАТУРЫ

1. Astakhova T., Kolbanev M., Krasnova A. Cyber-Physical Systems and Digital Twins as a Concept of Building the World of Intellectual Technologies and Management of Production Processes // Marketing and Smart Technologies. Smart Innovation, Systems and Technologies. Vol. 280. Singapore : Springer.\
2. Khajavi S, Hossein Motlagh N., Jaribion A., Christine Werner L. Digital twin: vision, benefits, boundaries, and creation for buildings // IEEE Access 7 (2019):147406-147419. October, 2019. DOI:10.1109/ACCESS.2019.2946515.
3. Боровков А. И., Рябов Ю. А., Марусева В. М. Новая парадигма цифрового проектирования и моделирования глобально конкурентоспособной продукции нового поколения // Цифровое производство: методы, экосистемы, технологии. МШУ СКОЛКОВО. 2018. С. 24–44. URL: http://assets.fea.ru/uploads/fea/news/2018/04_april/12/cifrovoe-proizvodstvo-032018.pdf. (20.06.2023).
4. Колбанев М. О., Яковлев С. А. Модели и методы оценки характеристик обработки информации в интеллектуальных сетях связи. СПб : СПбГУ, 2002. 230 с.

УДК 631.151

ЦИФРОВОЕ СЕЛЬСКОЕ ХОЗЯЙСТВО: НОВЫЕ ТЕХНОЛОГИИ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ И БЕЗОПАСНОСТИ В СЕЛЬСКОМ ХОЗЯЙСТВЕ

Маслов Никита Сергеевич
Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия
e-mail: j-knaginino@yandex.ru

Аннотация. В работе рассматриваются вопросы цифровой трансформации сельскохозяйственной отрасли. Предлагается архитектура цифрового сельского хозяйства, включающая в себя передовые цифровые технологии. Рассматриваются составляющие каждой из цифровых компонент.

Ключевые слова: цифровое сельское хозяйство; передовые технологии; цифровые компоненты; архитектура цифрового сельского хозяйства.

DIGITAL AGRICULTURE: NEW TECHNOLOGIES TO IMPROVE EFFICIENCY AND SAFETY IN AGRICULTURE

Maslov Nikita
Nizhny Novgorod State of Engineering and Economic University
22a Oktyabrskaya St, Knyaginino, 606340, Russia
e-mail: j-knaginino@yandex.ru

Abstract. The paper deals with the issues of digital transformation of the agricultural industry. The architecture of digital agriculture is proposed, which includes advanced digital technologies. The components of each of the digital components are considered.

Keywords: digital agriculture; advanced technologies; digital components; architecture of digital agriculture.

Понятие «Цифровая трансформация» за последние десятилетия стало неотъемлемой частью жизни общества. Цифровые инновации и технологии стремительно распространяются по всем сферам деятельности, позволяя ускорить процесс цифровой трансформации. Становится вполне очевидно, что наступила эпоха цифровой трансформации, которая связана с Четвертой промышленной революцией.

Четвертая промышленная революция, которую часто называют Индустрия 4.0 предполагает собой полную цифровую трансформацию всего производства. Переход на цифровое производство, характеризуется интеллектуальными системами, позволяющими управлять предприятием в режиме реального времени, используя технологии Интернета вещей (Internet of Things).

Цифровая трансформация отрасли сельского хозяйства в последние годы стала особо актуальна. Сельское хозяйство является основным сектором в мире, снабжающим продуктами питания людей по всему миру, внося огромный вклад в формирование мирового ВВП. Население стран растет, вместе с тем увеличиваются и потребности в продовольственных товарах, что подталкивает отрасль сельского хозяйства на модернизацию и переход на передовые технологии.

Необходимо отметить, что отрасль сельского хозяйства носит многоотраслевой характер, что подразумевает собой большой спектр различных технологий, с особенностями присущими определенной отрасли. Данный факт накладывает определенные ограничения на внедрение и использование цифровых технологий. Кроме этого, чтобы в полной мере перейти к модели цифрового сельского хозяйства, необходимо внедрять цифровые технологии и в малые хозяйствующие субъекты, что повлечет за собой дополнительные расходы для производителей.

Переход на цифровое сельское хозяйство включает в себя комплекс инновационных разработок, позволяющих адаптировать сельскохозяйственное производство под конкретные изменяющиеся условия окружающей среды, появление новых заболеваний и др.

Компоненты цифрового сельского хозяйства на всех этапах жизненного цикла сельскохозяйственного предприятия должны функционировать как единое целое. Достичь целостности функционирования позволяет архитектурный подход.

Согласно рекомендациям IEEE 1471–2000 архитектура системы это: «Фундаментальная организация системы, воплощенная в ее компонентах, их взаимоотношениях друг с другом и с окружающей средой, а также принципы, определяющие ее структуру и эволюцию» [1].

В общем виде архитектура представляет собой многоуровневую модель, включающую в себя совокупность компонентов системы, позволяя визуализировать взаимосвязь уровней между собой.

Цифровое сельское хозяйство прежде всего должно быть ориентированно на использование передовых технологий. Все статистические данные сельскохозяйственного производства должны быть интегрированы в одну общую цифровую платформу. Кроме этого, внедрение и развитие технологий Интернета вещей, робототехники и искусственного интеллекта позволит кардинально изменить способ сбора, обработки и использования данных производства. В работе представлена архитектура цифрового сельского хозяйства в общем виде. Компоненты цифрового сельского хозяйства:

– цифровая платформа сельского хозяйства;
– центр обработки данных;
– умное производство;
– умный склад;
– центр управления данными.

Цифровая платформа [2] собирает данные мониторинга сельскохозяйственных предприятий, дает доступ сельскохозяйственным организациям к отчетам аналитического центра, информирует о предстоящих мероприятиях в области цифрового сельского хозяйства.

Центр обработки данных представляет собой виртуальное хранилище данных, в котором происходит анализ и обработка данных, собранных в процессе мониторинга. На основе анализа данных фермеры смогут принимать обоснованные решения касающиеся улучшения эффективности производства, все данные мониторинга можно получить в режиме реального времени. В работе выделяются 4 вида мониторинга:

– мониторинг состояния почвы;
– мониторинг окружающей среды;
– мониторинг состояния животных;
– мониторинг состояния сельскохозяйственной техники.

Кроме этого, цифровое сельское хозяйство включает в себя технологии умного производства состоящее из точного земледелия и точного животноводства и технологий умного склада, функции которого заключаются в хранении, переработке и сбыте продукции. Все вышеописанные составляющие реализуются при помощи инструментов Центра управления данными, использующих цифровые технологии, такие как:

– робототехника;
– датчики сбора данных; удаленная работа персонала;
– беспилотное управление сельскохозяйственной техникой и др.

Объединение цифровых технологий в одну единую систему позволяет не только улучшить качество продукции, но и даст возможность потребителю отследить весь жизненных цикл приобретаемого продукта.

Следует отметить, что архитектура цифрового сельского хозяйства отличается от эталонной сетевой модели OSI, так как компоненты цифрового сельского хозяйства не образуют собой линейный поток, как это принято в модели OSI. Помимо этого, некоторые компоненты архитектуры в той или иной сельскохозяйственной организации могут отсутствовать, например, если организация занимается только животноводством, то блок с точным земледелием, является не обязательным для этой организации.

Ещё одним немаловажным компонентом цифрового сельского хозяйства является технология блокчейн, позволяющая отследить всю цепочку поставки и сбыта сельскохозяйственной продукции. Использование данной технологии позволяет обеспечить продовольственную безопасность и прозрачность информации о происхождении продукции [3].

Таким образом, цифровое сельское хозяйство включает в себя 5 крупных компонент, подразумевающих собой использование передовых цифровых технологий. Использование компонент в совокупности обеспечит снизить производственные затраты, увеличить производство сельскохозяйственной продукции и обеспечить продовольственную безопасность.

СПИСОК ЛИТЕРАТУРЫ

1. IEEE 1471–2000 Recommended Practice for Architectural Description of Software–Intensive Systems [Electronic resource] URL: http://cabibbo.dia.uniroma3.it/ids/altrui/ieee1471.pdf (дата обращения 28.02.2023).
2. Астахова Т. Н., Колбанев М. О., Шамин А. А. Децентрализованная цифровая платформа сельского хозяйства //Вестник НГИЭИ. 2018. №. 6 (85). С. 5-17.
3. Кирилова Д. А., Маслов Н. С., Рейн А. Д. Blockchain как новая технология для разработки // International Journal of Open Information Technologies. 2019. Т. 7. № 1. С. 34-38.

УДК 517.98.519.2.629.039

О РОЛИ ФЕНОМЕНА АСИММЕТРИИ ВНУТРЕННЕГО ВРЕМЕНИ В ТЕОРИИ ДОЛГОВЕЧНОСТИ СЛОЖНЫХ ДИНАМИЧЕСКИХ СИСТЕМ

Острейковский Владислав Алексеевич, Сорочкин Андрей Викторович
Сургутский государственный университет
Ленина пр., 1, Сургут, 628412, Россия
e-mails: ova@surgu.ru, sorochkin_av@surgu.ru

Аннотация. Рассмотрены методы анализа феномена асимметрии внутреннего времени, используемые для построения теории долговечности сложных динамических систем.

Ключевые слова: долговечность, ресурс, неустойчивость, необратимые процессы, асимметрия внутреннего времени.

THE ROLE OF THE INTERNAL TIME ASYMMETRY PHENOMENON IN THE DURABILITY THEORY OF COMPLEX DYNAMIC SYSTEMS

Ostreikovskii Vladislav, Sorochkin Andrei
Surgut State University
1 Lenin Av., Surgut, 628412, Russia
e-mails: ova@surgu.ru, sorochkin_av@surgu.ru

Abstract. The methods of analysis of the phenomenon of asymmetry of internal time, used to build a theory of durability of complex dynamic systems, are reviewed.

Keywords: durability, resource, instability, irreversible processes, asymmetry of internal time.

В последние два столетия XX и XXI веков, в науке были получены большие достижения в области оценки показателей долговечности сложных систем. Однако, загадочный феномен «время» таит ещё много вопросов. И решение этой проблемы продолжает оставаться актуальным в современной науке. Человечество убедилось, что многие загадки феномена времени всё ещё ждут своего решения. Так, по меткому определению С.И. Ожегова, время является одной из самых загадочных форм объективно развивающейся материи, которая расставляет в природе всё по своим местам, и до сих пор продолжает оставаться много вопросов по этой проблеме.

Одной из таких нерешённых проблем является проблема асимметрии внутреннего времени сложных динамических систем. При этом следует отметить, что за последние два века человечество обогатило науку решением ряда задач в рассматриваемом направлении, в частности [1-4].

В приведённых работах получены следующие важные результаты:

1. Внутреннее время существует только для неустойчивых динамических систем. Если среднее внутреннее время ‹T› согласуется с динамическим временем t, например, в таких ситуациях как преобразование пекаря, то смешивать T и t нельзя, ибо понятия внешнего и внутреннего времени совершенно различны, хотя их можно измерять по наручным часам.

2. При анализе прогнозирования состояния сложной динамической системы является наиболее удовлетворительным рассмотрение их внутреннего описания необратимости путем отображения эволюции во времени с использованием полугруппы и перехода к вероятностным процессам, которые позволяют ввести делокализацию и в пространстве, и во времени (так называемому «овремениванию» пространства).

3. Так как в основе общей теории относительности лежит понятие четырёхмерного интервала ds2 и координаты в пространстве-времени, используемые для описания ds2, считаются произвольными, то в частном случае космологической модели с пространственными гиперповерхностями отрицательной кривизны можно ввести внутренне время, тесно связанное с обычным космическим временем. Хотя в общем случае такое утверждение неверно.

4. Поведение отдельных траекторий систем весьма чувствительно к начальным условиям. Но если воспользоваться преобразованием Λ и перейти к нелокальному описанию, то основное внимание будет сосредоточено не на поведении точек, а на поведении «малых» областей. В отличие от описания на языке траекторий нелокальное описание устойчиво. В этом случае такое утверждение неверно.

5. Состояния и законы находятся в тесной взаимосвязи. Существуют самосохраняющиеся формы начальных условий. Начальное условие приходится на момент времени, выбираемый произвольно. Он не обладает никакими специфическими свойствами, которые выделяли бы его среди прочих моментов времени. Из существования законов, ориентированных во времени, таких, как возрастание энтропии по направлению

к будущему, следует существование и такого рода состояний систем, ориентированных во времени. Следовательно, симметричное состояние должно возникать из другого симметричного состояния и со временем переходить в какое-то симметричное состояние. Аналогично, состояние с нарушенной симметрией должно возникать из однотипного состояния и со временем переходить в какое-то состояние того же типа.

6. Инвариантность характера состояний приводит к тесной взаимосвязи состояний и законов, т. е. взаимосвязи прошлого, настоящего и будущего. Настоящее связано с состояниями, будущее — с законами (уравнениями), по которым преобразуются состояния. Таким образом, если настоящее имеет ориентацию во времени, то и будущее будет обладать нарушенной временной симметрией.

7. Так как в природе выполняется второе начало термодинамики, которое применимо только к системам в значительной степени неустойчивым, то неустойчивость и необратимость тесно связаны между собой: необратимое, ориентированное время может появиться только потому, что будущее не содержится в настоящем.

8. В этом плане известные постулаты феномена времени А.А. Маркова, Н.М. Седякина и К. Шеннона [4] применимы только для класса устойчивых систем.

9. «Человек наделён внутренней стрелой времени. Стрела времени не противопоставляет человека природе. Наоборот, она свидетельствует о том, что человек является неотъемлемой составной частью эволюционирующей Вселенной. Время — ключ к пониманию истории человечества, как на уровне отдельной личности, так и на уровне общества. Время — ключ к пониманию природы [1].

Краткая характеристика основных направлений и трудно решаемых задач в проблеме «прошедшее-настоящее-будущее» применительно к обоснованию исходных остаточных ресурсов при оценке долговечности макроскопических технических систем на наш взгляд являются следующими.

– разработка математических методов анализа и количественной оценки асимметрии времени в теории прогнозирования состояния макроскопических сложных динамических систем на разных уровнях описания их жизненного цикла;

– разработка вычислительных методов для построения математических моделей анализа асимметрии времени;

– разработка информационных технологий, реализующих данные модели;

– разработка проекта фундаментального исследования в области развития и применения методов количественной оценки учета асимметрии времени в прогнозировании и достижении сроков проектной и запроектной эксплуатации высоко опасных и критически важных сложных динамических систем.

К перспективным и труднорешаемым проблемам в настоящее время следует отнести:

– разработка математических моделей анализа и количественной оценки асимметрии времени в теории прогнозирования состояния сложных макроскопических динамических систем;

– разработка и исследование проблемы прогнозирования и количественной оценки остаточного ресурса на всех уровнях «прошлое–настоящее–будущее» сложных технических критически важных систем;

– разработка вычислительных методов расчёта количественной оценки асимметрии времени сложных макроскопических динамических систем.

Данные направления исследований в итоге должны стать основой для разработки «Программы развития фундаментальных методов учёта асимметрии времени на всех этапах жизненного цикла сложных технических комплексов».

Трудно не согласиться с замечанием Ю.Л. Климонтовича в Заключении к книге И. Р. Пригожина «От существующего к возникающему: Время и сложность в физических науках»: «Значение и роль необратимых физических процессов для биологических систем были поняты значительно раньше, чем сформировалась современная статистическая и термодинамическая теория необратимых процессов. Основополагающими здесь являются работы В.И. Вернадского, и заложенные в них положения науки о биосфере уже содержали представления современной теории самоорганизации» [1].

СПИСОК ЛИТЕРАТУРЫ

1. Пригожин И. Р. От существующего к возникающему: Время и сложность в физических науках : пер. с англ. / Под ред. Ю. Л. Климонтовича. Изд. 2-е, доп. М. : Едиториал УРСС, 2002. 288 с.
2. Пригожин И. Р. Конец определенности. Время, хаос и новые законы природы. Ижевск: Ижевская республиканская типография. 1999. 216 с.
3. Острейковский В. А. Феномен асимметрии времени в теории неустойчивых и необратимых процессов сложных динамических систем : монография / Сургут. гос. ун-т. Сургут : Печатный мир, 2017. (Серия «25 лет СурГУ»).
4. Острейковский В. А., Денисова Т. Ю., Шевченко Е. Н. Асимметрия времени в теории прогнозирования состояния сложных динамических систем : монография Сургут. Печатный мир, 2018.

УДК 004.94

ПРИМЕНЕНИЕ МЕТОДА ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ДЛЯ РЕШЕНИЯ ЗАДАЧ СЕТЕВОГО ПЛАНИРОВАНИЯ

Пуха Геннадий Пантелеевич
Санкт-Петербургский государственный университет сервиса и экономики
наб. канала Грибоедова 30-32, лит. А, Санкт-Петербург, 191023, Россия
e-mails: pgp2003@list.ru

Аннотация. В докладе на примере одного из возможных вариантов процесса развертывания полевого узла связи рассматривается применение метода имитационного моделирования для решения задачи по оценки своевременности данного процесса и его оптимизации.

Ключевые слова: принятие решения, сетевое планирование, случайные продолжительности работ, нормальный закон, ограничения, имитационная модель, своевременность реализации проекта.

APPLICATION OF SIMULATION MODELING FOR SOLVING PROBLEMS OF NETWORK PLANNING

Puha Gennady
Saint Petersburg State University of Service and Economics
30-32 emb. Griboyedov Canal, letter A, St. Petersburg, 191023, Russia
e-mails: pgp2003@list.ru

Abstract. Using the example of one of the possible options for the deployment of a field communication center, the report discusses the use of the simulation method to solve the problem of assessing the timeliness of this process and optimizing it.

Keywords: decision making, network planning, random durations of work, normal law, constraints, simulation model, timeliness of project implementation.

Как известно, решение задач по управлению проектами, зачастую, связано с использованием аппарата, так называемого сетевого планирования (СП) [1], основанного на математическом аппарате теории графов и системного подхода для отображения и алгоритмизации комплексов взаимосвязанных работ, действий или мероприятий для своевременного и планомерного достижения четко поставленной цели.

Для отображения и алгоритмизации тех или иных действий или ситуаций в данном аппарате используются экономико-математические модели, которые принято называть сетевыми моделями или — *сетевые графики*. И, если временные параметры продолжительности выполнения отдельных работ комплекса являются детерминированными, то продолжительность так называемого «критического пути», состоящего из работ с детерминированными временными оценками просто определяется как их сумма.

Для расчета же параметров всей сети с вероятностными оценками продолжительностей работ наиболее широко применяется метод усреднения, суть которого состоит в том, что вероятностные оценки «превращают» в детерминированные и, вводя добавочную характеристику — меру неопределенности оценки — ее дисперсию, производят расчет параметров сетевого графика. При этом, на основании центральной предельной теоремы теории вероятностей принято считать, что распределение сроков наступления событий сетевого графика, в том числе завершающего со значением срока $T_{ожс}$ и его дисперсией $\sigma^2(T)$, подчинено нормальному закону. А поэтому и продолжительность критического пути, и его дисперсия могут быть также определены простым суммированием составляющих их средних и дисперсий.

Однако, следует всегда помнить, что предположение о нормальном законе распределения суммы случайных величин справедливо в том случае, если число слагаемых достаточно большое (порядка 10 [2]). Следовательно, наличие предположения о нормальном распределении значений отдельных операций существенно снижает адекватность сетевых моделей и накладывает определенные ограничения на область применения метода.

Снять же указанные ограничения аналитических моделей аппарата СП на законы распределения случайных величин исходных данных, по нашему мнению, позволяет метод имитационного моделирования (ИМ), так как соответствующие технологии его реализации имеют возможность задавать любые их варианты.

Решение. Так, на примере решения задачи, связанной с оценкой своевременности выполнения комплекса работ по развертыванию полевого узла связи (ПУС) можно показать [3], что сетевая модель данного процесса с высокой степенью адекватности реализуется алгоритмом имитационной модели, опять же, например, в специализированной среде GPSS Studio [4], а результаты серии экспериментов, выполненные с ее помощью, дают возможность не только оценить своевременность завершения всего процесса в целом, но и произвести его оптимизацию [5, 6].

Значительное число экспериментов, которое потребуется при этом провести, несомненно, является заметным препятствием практического применения метода ИМ. Однако развитие современных технологий его реализации помогают автоматизировать данную процедуру [3, 4].

Очевидно, что перераспределяя между исполнителями параллельных работ (как это и положено при сетевом планировании) их объемы, выравнивая при этом соотношения их временных интервалов, и выполняя аналогичные серии экспериментов можно:

– во-первых, существенно сократить критический путь выполнения поставленной задачи;
– во-вторых, найти условия, при которых она будет выполнена своевременно;
– и, в-третьих, определить какие из операций (процедур) оказывают наибольшее влияние на конечный результат и, поэтому требуют особого внимания с точки зрения риска их невыполнения при управлении «проектом».

Таким образом применение технологии имитационного моделирования в сочетании с методами сетевого планирования позволяет успешно решать задачи, связанные с поддержкой принятия решений по управлению организационно-техническими проектами.

СПИСОК ЛИТЕРАТУРЫ

1. Скугорев В. Д., Кудин Л. В. Сетевое планирование на флоте. М. : Воениздат, 1973. 248 с.
2. Вентцель Е. С. Исследование операций: задачи, принципы, методология. М. : Наука, 1988. С. 206.
3. Пуха Г. П. Моделирование систем: учеб. пособие СПб : СПбГЭУ, 2020. 279 с.

4. Девятков В. В., Девятков Т. В., Федотов М. В. Имитационные исследования в среде моделирования GPSSSTUDIO : учеб. пособие / под общ. ред. В. В. Девяткова. М. : Вузовский учебник : ИНФРА-М, 2018. 283 с.
5. Пуха Г. П. К вопросу об использовании системы поддержки принятия решений в работе пунктов управления связью флотов // Морская радиоэлектроника. № 2(72) июнь 2020. С. 10-13.
6. Котомин М. А., Пуха Г. П. Применение имитационного моделирования для поддержки принятия решения на организацию технического обслуживания производственных объектов // Актуальные проблемы защиты и безопасности : Труды XXV Всероссийской научно-практической конференции. СПб, 2022. С. 268-278.

УДК 004.056

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ИНФРАСТРУКТУРЫ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ С УЧЕТОМ БЕЗОПАСНОСТИ

Соколов Роман Владимирович
Санкт-Петербургский государственный экономический университет
канала Грибоедова наб.,30-32, лит. А., Санкт-Петербург, 191023, Россия
e-mail: rsok@rambler.ru

Аннотация. Рассматривается математическая модель выбора вариантов бизнес-процессов информационной инфраструктуры управления предприятиями с учетом обеспечения заданного уровня информационной безопасности.

Ключевые слова: информационная безопасность; коэффициент защищенности; математическая модель.

MATHEMATICAL MODEL OF CONFIDENTIAL INFORMATION SAFETY-CONSCIOUS ENTERPRISE MANAGEMENT

Sokolov Roman
Saint Petersburg State University of Economics
30-32 Griboedov canal Emb, St. Petersburg, 191023, Russia
e-mail: rsok@rambler.ru

Abstract. A mathematical model for selecting options for business processes of the information infrastructure of enterprise management is considered, taking into account the provision of a given level of information security.

Keywords: information security; security factor; mathematical model.

Обеспечение информационной безопасности в управлении предприятиями является актуальной проблемой, требующей дальнейших исследований с применением математических методов.

По мере возрастания уровня цифровизации общества повышается опасность экономических и прочих потерь, связанных с нарушениями в работе цифровых систем управления производственными компаниями [1].

Проектирование системы защиты информации должно соответствовать концепции безопасности системы защиты [2–5].

В области информационной безопасности используются следующие стандарты [5], которые анализируются в докладе.

Систематизированы возможные информационные угрозы и методы защиты по этапам обработки информации в системе управления производственной компанией.

Предлагаемая математическая модель информационной инфраструктуры управления предприятием позволяет сделать обоснованный выбор вариантов осуществления бизнес-процессов, входящих в состав задач управления предприятием. Структура линейной модели с двоичными переменными содержит критерий эффективности в виде минимума годовых приведенных затрат на информационную инфраструктуру и ограничения по времени, достоверности и информационной безопасности обработки информации по задачам. В качестве вариантов выбора анализируются варианты, основанные на прогрессивных сквозных информационных технологиях.

Раскрывается комплексный обобщенный показатель оценки качества инфраструктуры защиты информации (обобщенный коэффициент защищенности, показывающий уровень отражения атак по всей совокупности возможных угроз) [6].

Предлагается математическая модель информационной инфраструктуры управления предприятием, отличающаяся наличием ограничений по информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Национальная программа «Цифровая экономика Российской Федерации». URL: https://digital.gov.ru/uploaded/files/natsionalnaya-programma-tsifrovaya-ekonomika-rossijskoj-federatsii_NcN2nOO.pdf (2019 г.) (дата обращения: 26.09.2023).
2. Соколов Р. В. Оценка информационной защищенности и экономических потерь в системах управления производственной компании // Экосистема цифровой экономики. СПб. : СПбГЭУ, 2021. С.79-85.
3. Соколов Р. В. Оценка информационно-экономической безопасности в системе управления производственной компанией // XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 27-29 октября 2021 г. : Материалы конференции. СПб, 2021. С. 232.
4. Российские университеты в условиях цифровизации: математические и инструментальные методы оценки качества управления : монография / под общ. ред. В. Г. Халина. М. : Проспект, 2019. 896 с.
5. Соколов Р. В., Андреевский И. Л. Проектирование и эксплуатация информационных систем : учебник. СПб.: СПбГЭУ, 2017. 382 с.
6. Стельмашонок Е. В., Стельмашонок В. Л. Оценка эффективности инфраструктуры защиты информации и ее влияние на основные показатели производственно-хозяйственной деятельности предприятия // Защита информации в компьютерных системах : монография. СПб : СПбГЭУ, 2017. 163 с.

УДК 742.012

АНАЛОГИИ ПРЕДСТАВЛЕНИЯ ДАННЫХ. СРАВНЕНИЕ ВЕРБАЛЬНЫХ ВЕЛИЧИН: ЭКОНОМИКА, ПЛАНОВАЯ ЭКОНОМИКА, РЫНОЧНАЯ ЭКОНОМИКА

Ярошевич Людмила Ивановна
Санкт-Петербургский государственный институт кино и телевидения
Правды ул., 13, Санкт-Петербург, 191119, Россия
e-mail: Ludmila-arttech@rambler.ru

Аннотация. Сравнение терминологических величин: экономика, плановая экономика, рыночная экономика. Какие смысловые изменения придают прилагательные рыночная и плановая системе экономика?

Ключевые слова: обратная информационная связь; терминология экономики; план, рынок.

ANALOGIES OF DATA REPRESENTATIONS. COMPARISON OF VERBAL QUANTITIES: ECONOMY, PLANNED ECONOMY, MARKET ECONOMY

Yaroshevich Ludmila
The St. Petersburg State institute of film and television
13 Pravda str., St. Petersburg, 191119, Russia
e-mail: Ludmila-arttech@rambler.ru

Abstract. Verbal values are compared: economy, planned economy, market economy. What semantic changes do the adjectives market and planned attach to the status term economy?

Keywords: feedback; terminology of economy; plan, market.

Экономика в переводе с греческого языка означает управление хозяйством, в записи это — сбалансированная система с множеством подчиненных параметров, участвующих в процессе исполнения.

Название Плановая экономика констатирует факт, что объемный документ, государственной важности, выполняется по всем правилам представления данных, в соответствии с фазовой диаграммой экономического развития и ожидаемым результатом выполнения алгоритма. План это — способ представления информации полного цикла. План помогает восприятию большого объема информации, в краткие сроки и правильной последовательности. Устройства текстов, инструкций по использованию техники, рецептов, списков, расписаний имеют аналогичный внутренний порядок, приспособленный для человеческого восприятия.

Современная борьба с Плановой экономикой похожа на борьбу с «ветряными мельницами». Те, кто говорят, что плановая экономика советского периода себя не оправдала, ссылаются на некоторый дефицит производства товаров потребления. Однако, дефицит товаров не имеет никакого отношения к закону о представления данных (плану), основанному на физиологии восприятия и передачи информации.

Обратимся к аналогам плана в разных сферах. Итак, можно ли себе представить музыку без партитуры, градостроительство без генплана, образование без учебных планов, судоходство без навигации и т.д., ведь план это и есть навигатор! Пространственная перспектива и время также присутствуют в каждом плане. Оппозиция всеми силами пытается «удружить» превратив, перспективный план в беспомощный и безрезультатный, кроме того, бесправный на международном уровне. Экономика должна быть плановой, потому как, любое намерение (цель) это — план.

Рыночная экономика. Система Экономика это — целый комплекс производственных отношений, внутри которого рынок представляет собой одну из соподчиненных частей. В фазовой диаграмме Экономика существует терминологическая иерархия между системой и подсистемами. Если мы, перед собирательным существительным Экономика напишем прилагательное рыночная, то понятие Рыночная экономика будет означать, что все хозяйственные отношения сводятся только к рынку. Экономика и рыночная экономика остаются в соотношении величин как целое и часть, подчиненная этой системе. Экономика — система, а в словосочетании рыночная экономика становится подсистемой. Аналогичные примеры: музыка и фортепьянная музыка; транспорт и транспортное средство; образование и среднее образование; экономика и экономика промышленности, … [1, 2].

В этой ситуации, т.н. рыночная (сырьевая) экономика составляет реальную угрозу системной величине Экономика. Кроме того, если, доля рыночной экономики будет возрастать, то по достижению критической точки, про Экономику можно будет уже не вспоминать, ее не будет…

Экономика это — сбалансированное сложное устройство, в котором царит установленный порядок (по крайней мере, должен царить), и это также важно, как охранять устройства технических сооружений, машин и приборов. Специалисты системотехники, занимающиеся «Вопросами организации и эксплуатации больших систем» удивляются, почему эта методология не получила распространения в области организации и управления в Экономике и государственном устройстве [1].

Какие бы сегодня названия Экономике не придумывали (рыночная, сырьевая), она была, есть и будет Плановой экономикой. Потому что план это — структура представления данных сложных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. М.: Издательство «АЗЪ», 1995.
2. Деревянко И. Что такое системотехника? // Проза.ру : сайт. URL: https://proza.ru/2019/10/01/1050 (дата обращения: 01.10.2023).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТРАНСПОРТНЫХ СИСТЕМ

УДК 65.011.5

ПРИМЕНЕНИЕ ERP- И MES-СИСТЕМ В СУДОСТРОИТЕЛЬНОЙ ОТРАСЛИ

Антонова Алёна Евгеньевна[1], Соколов Сергей Сергеевич[2]
[1]Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
[2]Российский университет транспорта (МИИТ)
Октябрьский пер., 7, Москва, 127018, Россия
e-mails: vasalen2@rambler.ru, sokolovss@gumrf.ru

Аннотация. Рассматриваются две основные системы автоматизации в судостроении (ERP и MES), применение которых является необходимым условием для успешного развития судостроительной отрасли.

Ключевые слова: судостроительная отрасль; системы управления; оптимизация производственных процессов; ресурсы предприятия; качество.

APPLICATION OF ERP- AND MES-SYSTEMS IN THE SHIPBUILDING INDUSTRY

Antonova Alena[1], Sokolov Sergey[2]
[1] Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
[2] Russian University of Transport (MIIT)
7 Oktyabrsky Av, Moscow, 127018, Russia
e-mails: vasalen2@rambler.ru, sokolovss@gumrf.ru

Abstract. Two main automation systems in shipbuilding (ERP and MES) are considered, the use of which is a necessary condition for the successful development of the shipbuilding industry.

Keywords: shipbuilding industry; control systems; optimization of production processes; enterprise resources; quality.

В судостроении используются две основные системы автоматизации: ERP (Enterprise Resource Planning) и MES (Manufacturing execution system). ERP-система предназначена для управления всеми ресурсами предприятия, включая финансы, продажи, производство и закупки. Она помогает оптимизировать бизнес-процессы, сократить издержки и улучшить качество продукции [1]. MES-система, наоборот, предназначена для автоматизации производственных процессов на предприятии.

Процессы судостроения могут быть описаны в ERP-системе следующим образом [2]:

– Планирование производства: составление графиков производства, расчет необходимых материалов и ресурсов, определение сроков выполнения работ.

– Управление заказами: прием заказов от клиентов, отслеживание их исполнения, контроль за выполнением сроков и качества работ.

– Учет материалов: учет поступления материалов, их расхода и остатков на складах.

– Расчет заработной платы: расчет заработной платы работников, учет налогов и отчислений.

– Отчетность: формирование отчетов о выполнении планов, состоянии запасов, финансовых показателях.

MES-системы в судостроении могут использоваться для автоматизации процессов управления производством, учета затрат и контроля качества продукции. Например, MES-системы позволяют:

– контролировать производственные процессы и управлять складом материалов;
– вести учет затрат на производство;
– формировать отчеты о производительности и затратах;
– интегрироваться с другими системами для обеспечения более эффективной работы.

Использование MES-систем позволяет снизить затраты на производство и повысить качество продукции, что в свою очередь может привести к увеличению конкурентоспособности предприятия и улучшению его финансовых показателей [3].

В судостроении ERP- и MES-системы играют важную роль в управлении производственными процессами и повышении эффективности работы предприятия. ERP-системы автоматизируют учет и управление финансами, заказами и производством, а MES-системы обеспечивают контроль над производственными процессами, учет материалов и затрат, а также формирование отчетов.

Таким образом, обе системы играют важную роль в повышении эффективности судостроения и улучшении качества продукции. Их сочетание позволяет более точно и оперативно управлять производственными процессами, что способствует повышению конкурентоспособности судостроительных предприятий. Внедрение ERP- и MES-систем является необходимым условием для успешного развития судостроительной отрасли.

СПИСОК ЛИТЕРАТУРЫ

1. Лилеев П. Типовые модели интеграции SAP: ERP и MES. Ч. 2. Современные подходы к интеграции ERP и MES на металлургических предприятиях // Информационные технологии. М., 2005. № 1. С. 90-93.
2. О'Лири Д. ERP системы. Современное планирование и управление ресурсами предприятия. Выбор, внедрение и эксплуатация / Пер. с англ. Водянова Ю.И. М. : Вершина, 2004. 372 с.
3. Андреев Е. Б., Куцевич И. В., Куцевич Н. А. MES-системы: взгляд изнутри. М. : РТСофт, 2015. 238 с.

УДК 681.5

МОДЕЛИРОВАНИЕ БЕЗОПАСНЫХТРАНСПОРТНЫХ СИСТЕМ УПРАВЛЕНИЯ

Голоскоков Константин Петрович, Астапкович Алексей Александрович, Коротков Виталий Валерьевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: goloskokovkp@gumrf.ru, kafkoib@gumrf.ru, korotkovvv@gumrf.ru

Аннотация. Рассматриваются методологические аспекты создания безопасных автоматизированных систем моделирования. Решение задач повышения эффективности принятия управленческих решений с целью оптимизации на основе моделирования в рамках АСУ транспортно-технологическим процессом.

Ключевые слова: Математическая модель; безопасная автоматизированная система; транспортно-технологический процесс; проблемно-ориентированный подход.

SIMULATION OF SAFE TRANSPORT CONTROL SYSTEMS

Goloskokov Konstantin, Astapkovich Alexey, Korotkrv Vitaly
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, Saint-Petersburg, 198035, Russia
e-mails: goloskokovkp@gumrf.ru, kafkoib@gumrf.ru, korotkovvv@gumrf.ru

Abstract. Methodological aspects of creating safe automated modeling systems are considered. Solving problems of increasing the efficiency of managerial decision-making in order to optimize based on modeling within the automated control system of the transport and technological process.

Keywords: Mathematical model; secure automated system; transport and technological process; problem-oriented approach.

Проведенные исследования показывают, что безопасные автоматизированные системы, как правило, обладают достаточно сложной эшелонированной структурой с взаимозависимыми звеньями и разнообразными функциями. Изучение таких систем с помощью аналитических методов затруднительно, поэтому возрастает актуальность разработки эффективных имитационных моделей для анализа и нормирования технико-экономических показателей функционирования системы материально-технического обеспечения.

Решением данной проблемы является создание прикладного математического обеспечения автоматизированной системы моделирования, предназначенной для автоматизации процессов анализа и функционирования на основе применения средств имитационного моделирования и принятия решений, а также вычислительной техники [1-5].

Таким образом, использование проблемно ориентированного подхода при создании АСУ позволяет снизить трудоемкость ее разработки и реализации, обеспечить возможность с единых методологических позиций унифицировать не только алгоритмы решения задач, но и применить стандартные методы обработки результатов решения задач.

Качественное исследование системы материально технического обеспечения основывается на создании проблемно-ориентированных автоматизированных систем. Для их разработки наиболее целесообразно использовать модельно ориентированный подход, позволяющий снизить трудоемкость разработки и реализации ее концептуальной, математической и алгоритмической моделей. Построение концептуальной модели в виде сети фреймов обеспечивает применение стандартных средств общения с пользователем системы и снижает требования к их квалификации.

При создании математической модели наиболее целесообразно выбрать представление процессов материально технического обеспечения в виде систем с типовой математической схемой.

СПИСОК ЛИТЕРАТУРЫ

1. Голоскоков К. П. Прогнозирование и оценка технического состояния сложных систем // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Глобальная энергетика. СПб., 2008. № 1 (53). С. 164-168.
2. Малюк В. И., Голоскоков К. П. Методика оценки рационального распределения ограниченных инвестиций в развитие производственной системы региона // Вестник ИНЖЭКОНа. Серия: Экономика. СПб., 2009. № 1 (28). С. 51-60.

3. Брусакова И. А., Власов М. П., Голоскоков К. П. Информационные технологии в научных исследованиях высшей школы : монография. СПб., 2012.159 с.
4. Голоскоков К. П. Автоматизированная система испытаний в структуре системы управления качеством // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. СПб., 2008. № 6 (69). С. 116-120.
5. Голоскоков К. П. Прогнозирование и оценка технического состояния сложных систем // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. СПб., 2008. № 1 (53). С. 164-168.
6. Голоскоков К. П., Нестеренко Н. К., Чиркова М. Ю. Повышение эффективности деятельности производственного предприятия // Аудит и финансовый анализ. М., 2014. № 1. С. 331-335.
7. Брусакова И. А., Голоскоков К. П. Математическая модель функциональной надежности автоматизированных систем управления // Вестник ИНЖЭКОНа. Серия: Технические науки. СПб., 2010. № 8. С. 48-51.
8. Голоскоков К. П., Железняк М. В. Прогнозирование с применением теории распознавания образов // Вестник ИНЖЭКОНа. Серия: Технические науки. СПб., 2011. № 8. С. 114-118.
9. Goloskokov K., Korotkov V., Marley V., Knysh T. Assessment of technical means quality indicators for smart transport systems // Journal of Physics: Conference Seriesthis link is disabled. 2021. 2096(1). 012184.
10. Ильченко А. А., Акмайкин Д. А., Гамс А. В. Автоматизированный подход к решению задачи определения района эксплуатации морского автономного надводного судна // Вестник государственного университета морского и речного флота им. адмирала С. О. Макарова. СПб., 2022. Т. 14. № 4. С. 508-518.

УДК 004.942

ОПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЕЙ ДВИЖЕНИЯ АВТОНОМНОГО СУДНА ПРИ ПОМОЩИ ПРОГРАММНОГО ПАКЕТА MAPLE 12

Данилин Герман Владиславович, Соколов Сергей Сергеевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: t.101@mail.ru, sokolovss@gumrf.ru

Аннотация. В течение уже нескольких десятилетий на морском и речном флоте существует тенденция к снижению численности судовых экипажей и повышению автоматизации. Крупные судоходные компании взяли курс на развитие технологий безэкипажного судовождения, которые в настоящий момент сдерживает отсутствие универсальной математической модели, описывающей движение судна, обладающей приемлемой точностью. Данная работа описывает вычислительный эксперимент по расчету параметров движения судна, опыт которого может быть использован при разработке универсальной математической модели движения судна.

Ключевые слова: безэкипажное судно; математическая модель; модель Басина; Maple; расчет координат.

DETERMINATION OF THE MOTION INDICATORS OF AN AUTONOMOUS VESSEL USING THE MAPLE 12 SOFTWARE PACKAGE

Danilin German, Sokolov Sergey
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: t.101@mail.ru, sokolovss@gumrf.ru

Abstract. For several decades now, there has been a tendency in the marine and river fleet to reduce the number of ship crews and increase automation. Large shipping companies have embarked on the development of technologies for unmanned navigation, which are currently hampered by the lack of a universal mathematical model describing the movement of a vessel with acceptable accuracy. This work describes a computational experiment for calculating the parameters of ship movement, the experience of which can be used in the development of a universal mathematical model of ship movement.

Keywords: unmanned vessel; mathematical model; Basin model; Maple; coordinate calculation.

Начиная со второй половины прошлого века и по настоящий момент разработкой математических моделей, описывающих движение судна, занималось не мало отечественных и зарубежных ученых [1-3]. Их труды обобщает то, что для краткого описания любой математической модели движения судна может быть использована одна и та же система формул [1], а отличие моделей друг от друга заключается в способе вычисления сил и коэффициентов, воздействующих на судно. На основании этого у каждой модели возникают достоинства и недостатки, делающие её пригодной для применения только в отношении судна определенного типа и конкретных условий плавания. При этом, универсальной модели пока еще не существует, хотя наибольший потенциал в разработке такой модели имеют нелинейные модели движения судна, такие как модель А. П. Тумашика, который разработал свою модель на основе модели А. М. Басина.

Проведение вычислений. В рамках данной работы с помощью среды «Maple 12» был произведен расчет параметров движения судна. Вычисления производились в том числе и с использованием систем уравнений, описывающих модель движения судна, предложенную А. М. Басиным.

В первую очередь были вычислены значения промежуточных величин, благодаря чему стало возможным решить дифференциальные уравнения и получить значения искомых величин.

На следующем шаге изначальный алгоритм вычисления был записан в цикл, осуществляющий 60 итераций. Результаты вычислений, полученные на каждой итерации, вносились в соответствующие массивы,

на основании значений которых были построены графики, наглядно отображающие зависимость искомых величин от времени.

После нахождения координат центра масс судна модель А. М. Басина была дополнена формулами, позволяющими определить координаты габаритной точки судна, наиболее удаленные от центра его масс, поскольку судно не является материальной точкой, и этот факт необходимо учитывать при прохождении судна в условиях ограниченного пространства, например, в канале или проливе, а также при расхождении с другими судами.

Далее в ходе работы были сформированы 4 новых массива, в которые вносились данные с учетом дополнений, вносимых добавленными формулами. По данным, хранимым в массивах, также были построены наглядные графики.

В результате произведенных вычислений были сформированы массивы данных, на основании которых были построены графики, наглядно отображающие изменение координат центра масс судна, его курсового угла, угла дрейфа, угловая и линейной скорости. Были сформированы массивы данных, на основании которых были построены графики, наглядно отображающие коридоры изменения координат выступающих за центр масс габаритных точек судна.

СПИСОК ЛИТЕРАТУРЫ

1. Юдин Ю. И., Сотников И. И. Математические модели плоскопараллельного движения судна. Классификация и критический анализ // Вестник МГТУ. Труды Мурманского государственного технического университета. Мурманск, 2006. Т. 9. № 2. С. 200-208.
2. Буцанец А. А. Разработка предложений по типовой структуре системы дистанционного управления беспилотным техническим флотом // Транспортное дело России. М., 2019. № 4. С. 100-103.
3. Данилин Г. В. Исследование математических моделей движения судна и технологий безэкипажного судовождения // Сборник научных статей национальной научно-практической конференции профессорско-преподавательского состава ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова». Т. 1. СПб., 2022. С. 72-78.

УДК 681.5, 004.9

БЕЗОПАСНАЯ СИСТЕМА МОНИТОРИНГА РАЗЛИВОВ НЕФТИ С ИСПОЛЬЗОВАНИЕМ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Егорова Кристина Вадимовна, Соколов Сергей Сергеевич
Государственный университет морского и речного флота им. адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: natashov1397@mail.ru, sokolovss@gumrf.ru

Аннотация. Использование беспилотных летательных аппаратов при мониторнге разливов нефти вместе с преимуществами: повышение эффективности, скорости и точности обнаружения, добавляют необходимость обеспечения информационной безопасности передачи и хранения информации. В данной статье рассматриваются основные угрозы и меры безопасности в данном контексте.

Ключевые слова: беспилотные летательные аппараты; мониторинг; безопасность данных.

SAFE SYSTEM FOR OIL SPILL MONITORING USING UNMANNED AERIAL VEHICLES

Egorova Kristina, Sokolov Sergey
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, Russia, 198035
e-mails: natashov1397@mail.ru, sokolovss@gumrf.ru

Abstract. The use of unmanned aerial vehicles for monitoring oil spills, along with the advantages of increasing the efficiency, speed and accuracy of detection, add the need to ensure information security in the transmission and storage of information. This article discusses the main threats and security measures in this context.

Keywords: unmanned aerial vehicles; monitoring; data security.

Обеспечение информационной безопасности в контексте модели поиска аварийных разливов нефти и нефтепродуктов группой беспилотных летательных аппаратов является критическим аспектом данной задачи. В свете возрастающей угрозы кибератак и несанкционированного доступа к данным, осуществление безопасной обработки и хранения информации становится необходимостью.

Преимущества использования беспилотных летательных аппаратов в задачах поиска разливов нефти включают повышение эффективности, скорости и точности обнаружения. Однако, с ростом автоматизации и сетевого взаимодействия, увеличивается и потенциальная уязвимость системы к различным видам атак.

Основные угрозы информационной безопасности в данном контексте включают несанкционированный доступ к данным, утечку информации, неправомерное использование и изменение данных, а также возможные атаки на инфраструктуру системы. Для предотвращения данных угроз, необходимо применять соответствующие меры безопасности.

Одним из ключевых аспектов безопасности является обеспечение конфиденциальности и целостности данных [1]. Это достигается путем применения шифрования данных, контроля доступа и мониторинга активности пользователей. Эффективная физическая защита инфраструктуры системы также является важным аспектом безопасности.

Важной частью безопасности данных является создание резервных копий и установка процессов восстановления данных в случае возникновения инцидентов безопасности. Это позволяет минимизировать потерю информации и обеспечить бесперебойную работу системы.

Тестирование на проникновение и аудит безопасности являются важными инструментами для выявления уязвимостей системы и анализа ее безопасности. Регулярное проведение этих процедур помогает выявить уязвимости и принять меры для их устранения [2].

Соответствие нормативным требованиям и стандартам безопасности, таким как ISO 27001 и GDPR, также является важным аспектом безопасности. Соблюдение этих нормативных требований помогает обеспечить высокий уровень безопасности информации.

Наконец, важно иметь план реагирования на инциденты безопасности, который включает установку процедур обнаружения, анализа и реагирования на угрозы безопасности. Это помогает эффективно и оперативно справиться с возможными инцидентами и минимизировать их воздействие.

Все эти аспекты необходимо учитывать для обеспечения информационной безопасности в контексте модели поиска аварийных разливов нефти и нефтепродуктов с помощью беспилотных летательных аппаратов [3-5]. Высокий уровень безопасности данных является гарантией эффективной работы системы и устойчивости к различным угрозам.

СПИСОК ЛИТЕРАТУРЫ

1. Нырков А. П., Вайгандт Н. Ю. Контроль целостности данных при мониторинге транспортных средств // Журнал университета водных коммуникаций. 2013. С. 54–61.
2. Нырков А. П., Рудакова С. А. Методика аудита объектов информатизации по требованиям информационной безопасности // Журнал университета водных коммуникаций. СПб., 2012. № 3. С. 146–149.
3. Егорова К. В. Имитационная модель управления полетом группы беспилотных летательных аппаратов на основе алгоритма пчелиной колонии // Вестник Воронежского государственного технического университета. В., 2023. Т.1. № 2. С. 68-71.
4. Егорова К. В., Соколов С. С., Гаскаров В. Д. Автоматизированная идентификация разливов нефти при помощи группы беспилотных летательных аппаратов // Сборник научных статей национальной научно-практической конференции профессорско-преподавательского состава ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова». СПб., 2022. С. 96-102.
5. Egorova K. V., Sokolov S. S., Knish T. Exploring the use of unmanned aerial vehicles for automated oil spill identification // E3S Web of Conferences 363, 01032. 2022.

УДК 004.032

МОДЕЛИ ПРОЦЕССА ОБРАБОТКИ ИНФОРМАЦИИ

Зубанова Анастасия Александровна, Когтев Алексей Валерьевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: nasty213@mail.ru, xx.ww.zz@ya.ru

Аннотация. Рассматриваются модели процесса обработки информации и проводится анализ их преимуществ и недостатков.

Ключевые слова: модели процесса обработки данных; скорость обработки; отказоустойчивость; сервер; надежность.

MODELS OF INFORMATION PROCESSING

Zubanova Anastasia, Kogtev Alexey
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: nasty213@mail.ru, xx.ww.zz@ya.ru

Abstract. Information processing models are considered and their advantages and disadvantages are analyzed.

Keywords: data processing models; processing speed; fault tolerance; server; reliability.

Обработка информации в настоящее время проводится повсеместно, будь то маленький магазин на окраине или же крупная компания на мировом рынке. Под обработкой информации понимается систематическое выполнение операций над данными, представляющими предназначенную для обработки информацию [1]. От выбора системы обработки информации зависит многое: скорость и качество обработки, защита обрабатываемых данных как от внешних злоумышленников, так и от случайной утечки, возможность производить обработку удаленно и т.д. Поэтому при выборе такой системы необходимо понимать, на основе какой модели она реализована.

Первой будет рассмотрена модель распределенной обработки информации [2, 3]. Процесс обработки информации в рамках такой модели производится на распределенных в локальной сети системах. Обычно такое распределение осуществляется с помощью специального инструментария, как правило, с применением соответствующего программного обеспечения. Процесс обработки делится на несколько самостоятельных блоков. Взаимодействие между компонентами системы обработки информации осуществляется одним из двух вариантов: удаленный вызов процедур или электронная почта [4]. Удаленный вызов процедур характеризуется прозрачностью, высокой скоростью отклика, но в то же время является достаточно дорогостоящим, поскольку

все сервера, участвующие в обработке, должны быть доступны на протяжении всего времени обработки информации и передачи ее между компонентами системы.

Далее рассмотрим модель обработки информации в рамках одного сервера/персонального рабочего места. В рамках данной модели обработка происходит в рамках одного сервера. Такая модель в современном обществе малоприменима, поскольку в нынешней ситуации преобладает многопользовательская обработка, при которой данные доступны с нескольких рабочих мест. Также данная модель не является надежной, поскольку при нарушении работоспособности сервера/персонального рабочего места, на котором происходит обработка, высока вероятность утраты обрабатываемой информации, что является неприемлемым [5].

Модель клиент/сервер заключается в том, что хранение, администрирование и предоставление конечной информации пользователям организуется на сервере [6]. Использование данных непосредственно пользователем происходит на клиенте. Модель централизованной обработки информации отличается от модели клиент/сервер тем, что при централизованной обработке информации предоставление конечной информации распределяется через порты/каналы ввода-вывода, а при использовании модели клиент/сервер распределение происходит через сетевые средства. Достоинством модели клиент/сервер, в первую очередь, является возможность установки гибких рабочих мест, в частности, гибкость заключается в разнообразии используемых платформ, операционных систем и т.д.

Итак, для первой модели преимуществом будет скорость отклика и прозрачность в рамках всей системы, также преимуществом будет отказоустойчивость, главным недостатком данной модели является высокая стоимость реализации. Что касается второй модели, преимуществом опять же будет являться скорость обработки, а также заметно меньшая стоимость реализации, но недостатки существенны. К ним относятся ненадежность, высокая вероятность утраты информации при наличии любого фактора, способного вывести из строя рабочее место, где установлена система. К преимуществам третьей модели можно отнести гибкость и отказоустойчивость, к недостаткам — возможное уменьшение скорости обработки информации. На основе этого можно сделать вывод, что в текущих реалиях модель клиент/сервер наиболее привлекательна для использования.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 15971—90 Системы обработки информации. Термины и определения. М. : Издательство стандартов, 1991. 12 с.
2. Информационные сети и телекоммуникационные каналы. Модель распределённой обработки информации [Электронный ресурс] // Bourabai Research. URL: http://bourabai.ru/telecom/nets17.html (дата обращения: 29.06.2023).
3. Ныркова А. П., Воеводский К. С., Князева К. О. Использование автоматизированной системы управления предприятием при территориально распределённом характере предприятия // Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». Санкт-Петербург, 26-28 октября 2016 : материалы конференции. СПб.: СПОИСУ, 2016. С. 528-529.
4. Mathematical Models for Solving Problems of Reliability Maritime System / Nyrkov A. [and others]. // Lecture Notes in Electrical Engineering, V. 442. 2018. Pp. 387-394.
5. Ныркова А. П., Ныркова А. А., Соколов С. С., Шнуренко А. А. Обеспечение безопасности объектов информатизации транспортной отрасли. СПб. : Изд-во Политехн. ун-та, 2015. 544 с.
6. Коржов В. Многоуровневые системы клиент-сервер [Электронный ресурс] // Сети/Network world. URL: https://www.osp.ru/nets/1997/06/142618 1997 (Дата обращения: 29.06.2023).

УДК 004.89 : 656.078

СОЗДАНИЕ БЕЗОПАСНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ТРАНСПОРТНОЙ ЛОГИСТИКИ НА ОСНОВЕ МУЛЬТИАГЕНТНОГО ПОДХОДА

Искандеров Юрий Марсович
СПИИРАН – СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: iskanderov_y_m@mail.ru

Аннотация. В статье рассмотрен мультиагентный подход, обеспечивающий создание безопасных информационных систем транспортной логистики с учетом существующих особенностей. Указанный подход позволяет эффективно реализовать актуальные требования по безопасности в интегрированных информационных системах, отражающих существующую топологию транспортных сетей и дальнейшее их развитие.

Ключевые слова: безопасная информационная система; транспортная логистика; интегрированная информационная система; мультиагентные технологии; мультиагентные системы.

CREATION OF SECURE INFORMATION SYSTEMS FOR TRANSPORT LOGISTICS BASED ON MULTI-AGENT APPROACH

Iskanderov Yury
SPIIRAS – SPCRAS
39 V.I. 14-th Line, St. Petersburg, 199178, Russia
e-mail: iskanderov_y_m@mail.ru

Abstract. The article discusses a multi-agent approach that ensures the creation of secure transport logistics information systems taking into account existing features. This approach makes it possible to effectively implement current security requirements in integrated information systems that reflect the existing topology of transport networks and their further development.

Keywords: secure information system; transport logistics; integrated information system; multi-agent technologies; multi-agent systems.

Известно, что отличительной особенностью объектов управления транспортно-технологических процессов (ТТП) является их распределенность в пространстве, иерархически-сетевой принцип организации управления и влияние факторов различной природы на качество предоставляемых услуг [1-4]. В связи с этим развитие инфотелекоммуникационной инфраструктуры на транспорте требует новых принципов построения интегрированных информационных систем (ИИС), отражающих существующую топологию транспортных сетей и дальнейшее их развитие. Такими новыми принципами являются принципы распределенных способов обработки информации.

Для успешной реализации целей цифровизации транспортно-логистические предприятия (ТЛП) должны обладать динамически перестраиваемыми информационными и телекоммуникационными системами. Ключевым решением этой проблемы является применение новых технологий, основной целью которых является интеграция гетерогенных приложений в распределенную инфраструктуру и создание гибких перестраиваемых безопасных информационных систем [5, 6].

Следует отметить, что современные достижения в области инфокоммуникаций, а именно мультиагентные технологии (МАТ), позволяют одновременно обеспечить учет необходимости реализации единства управления транспортом с особенностями распределенного, сетевого построения структуры, поскольку обладают соответствующими возможностями [7-9].

Каждый агент является уникальной сущностью в рамках мультиагентной системы (МАС) и имеет глобальное уникальное имя. Данное имя является постоянным, т.е. не изменяется в процессе миграции агента. Указанное свойство позволяет в любых условиях выполнить корректную идентификацию агента.

Применение МАТ позволяет эффективно реализовать актуальные требования по безопасности в ИИС [10-12]:

- обеспечение аутентификации клиента при удаленном создании агента;
- обеспечение взаимной аутентификации МАС;
- обеспечение аутентификации и передачи полномочий агента;
- обеспечение политики безопасности агента и МАС.

Поскольку МАС функционируют без вмешательства человека, следовательно, МАС, участвующие в процессе пересылки агента, проводят операцию взаимной аутентификации автоматически (т. е. например, без ввода пароля). Аутентификация агентов использует концепцию аутентификаторов. Аутентификатор — это алгоритм, который определяет аутентичность агента. Аутентификатор использует такую информацию, как аутентичность МАС или клиентского приложения, запустившего агента, а также данные об ответственных лицах агента и его агентской системы.

Подсистема безопасности в МАС также обеспечивает и аутентификацию неагентных приложений. Данная аутентификация может осуществляться с помощью паролей или смарт-карт.

Мультиагентный подход, положенный в основу формирования ИИС позволит кардинальным образом модернизировать организацию и повысить безопасность процессов функционирования ТЛП РФ. Ожидаемый результат такого подхода высокая эффективность, гибкость и надежность функциональных подсистем и их системы управления в целом, способность обеспечить высокий уровень качества транспортных услуг, и как следствие, высокую конкурентоспособность на отечественном и мировом рынках.

СПИСОК ЛИТЕРАТУРЫ

1. Искандеров Ю. М. Особенности информатизации транспортно-технологических процессов в цепях поставок. Информатизация и связь. 2019. № 4. С. 31-37.
2. 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». СПб. : СПбПУ, 2016. С. 62-69.
3. 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. : СПбПУ, 2016. С.53-62.
4. Искандеров Ю. М., Свистунова А. С., Хасанов Д. С., Чумак А. С. Интеллектуальная поддержка принятия решений в логистических системах // Морские интеллектуальные технологии. 2021. № 2-1 (52). С. 145-153.
5. Искандеров Ю. М. Информатизация транспортно-технологических процессов в цепях поставок // Системный анализ в проектировании и управлении. Сборник научных трудов XXVI Международной научно-практической конференции. В 3-х частях. СПб., 2023. С. 58-64.
6. Искандеров Ю. М. Интеграция информационных ресурсов для управления транспортными процессами: системные аспекты // Системный анализ в проектировании и управлении. сборник научных трудов XXV Международной научной и учебно-практической конференции : в 3 ч. СПб., 2021. С. 254-260.
7. Искандеров Ю. М. Мультиагентные системы для управления логистическими функциями в цепях поставок // Логистика: современные тенденции развития. Материалы XVIII Международной научно-практической конференции. 2019. С. 219-221.
8. Iskanderov Y., Pautov M. Actor-network approach to self-organisation in global logistics networks. Studies in Computational Intelligence. 2020. Т. 868. С. 117-127.
9. Iskanderov Y., Pautov M. Agents and multi-agent systems as actor-networks // ICAART 2020 — Proceedings of the 12th International Conference on Agents and Artificial Intelligence. 2020. 12. С. 179-184.
10. Искандеров Ю. М., Паутов М. Д. Защита корпоративной информации в транспортно-логистических сетях // Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. 2017. С. 275-276.
11. Искандеров Ю. М., Паутов М. Д. Интеллектуализация обеспечения информационной безопасности при управлении цепями поставок // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция : Материалы конференции. СПб. ,2022. С. 273-274.
12. Iskanderov Y., Pautov M. Security of information processes in supply chains. Advances in Intelligent Systems and Computing. 2019. Т. 875. С. 13-22.

УДК 004.89 : 656.078

ПОДСИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ ПЕРЕВОЗКИ НЕГАБАРИТНЫХ ГРУЗОВ

Искандеров Юрий Марсович[1], Чумак Александр Сергеевич[2], Шахнов Сергей Федорович[2]
[1] СПИИРАН – СПб ФИЦ РАН
В. О. 14 линия, 39, Санкт-Петербург, 199178, Россия
[2] ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова»,
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: iskanderov_y_m@mail.ru, chumak@nst-spb.ru, sfshah@yandex.ru

Аннотация. В статье рассмотрена подсистема информационной безопасности интеллектуальной поддержки перевозки негабаритных грузов, учитывая существующие особенности такой перевозки. Показано, что первоочередное внимание необходимо уделить защите информации, размещенной в базе знаний интеллектуальной системы поддержки принятия решений. Определены основные задачи подсистемы информационной безопасности. Отмечена необходимость комплексного использования релевантных методов защиты информации.

Ключевые слова: подсистема информационной безопасности; интеллектуальная поддержка; негабаритный груз; перевозка; база знаний; методы защиты информации.

INFORMATION SECURITY SUBSYSTEM FOR INTELLIGENT SUPPORT FOR TRANSPORTATION OF OVERSIZED CARGO

Iskanderov Yury[1], Chumak Alexandr[2], Shakhnov Sergey[2]
[1]SPIIRAS – SPCRAS
39 V.I. 14-th Line, St. Petersburg, 199178, Russia
[2]Admiral Makarov State University of Maritime and Inland Shipping,
5/7, Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: iskanderov_y_m@mail.ru, chumak@nst-spb.ru, sfshah@yandex.ru

Abstract. The article discusses the information security subsystem for intellectual support for the transportation of oversized cargo, taking into account the existing features of such transportation. It is shown that priority attention must be paid to the protection of information located in the knowledge base of an intelligent decision support system. The main tasks of the information security subsystem are defined. The need for integrated use of relevant information security methods is noted.

Keywords: information security subsystem; intellectual support; oversized cargo; transportation; knowledge base; information security methods.

В современных условиях для успешной реализации транспортировки негабаритных грузов необходимо использовать защищенную интеллектуальную систему поддержки принятия решений (ИСППР) [1-10]. Сведения, которые будут сформированы и использованы в ИСППР, 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 ИСППР также является актуальным и важным [11-13]. Первоочередное внимание необходимо уделить защите информации, размещенной в базе знаний (БЗ), в которой содержится вся ключевая информация о выполненных и планируемых к выполнению проектах транспортировки негабаритных грузов. Обеспечение указанной защиты целесообразно возложить на подсистему информационной безопасности (ПИБ) в составе ИСППР.

Основными задачами ПИБ являются [14]:

– Контроль доступа к данным для авторизованных пользователей.
– Контроль доступа к информационным услугам, функциям поиска и интеллектуального анализа данных.
– Гарантия подлинности и целостности информации, ее защита от несанкционированного изменения или уничтожения.
– Защита конфиденциальности.
– Определение и разъяснение всех сомнений относительно правил информационного обеспечения сотрудничества.

Для реализации ПИБ необходимо использовать как традиционные методы защиты информации, такие как: постановка на учет; протоколирование; аутентификация; идентификация; контроль доступа; межсетевые экраны; криптография, так и методы прикладной психологии, направленные на обнаружение потенциальных утечек данных о персонале, известные как методы профилирования, интегрированные со специализированным программным обеспечением DLP (Data Loss Prevention) и SIEM (Security information and event management) [14].

Комплексное использование различных средств информационной безопасности позволяет повысить надежность функционирования ИСППР в целом и обеспечить уверенность в эффективности принимаемых решений.

СПИСОК ЛИТЕРАТУРЫ

1. Искандеров Ю. М. Построение моделей интегрированной информационной системы транспортной логистики на основе мультиагентных технологий // Международная научно-практическая конференция «Новая экономика и основные направления ее формирования» : сб. статей. СПб. : СПбПУ, 2016. С. 62-69.

2. Искандеров Ю. М., Дорошенко В. И. Организация транспортно-технологических процессов на основе интегрированных информационных систем // Международная научно-практическая конференция «Новая экономика и основные направления ее формирования» : сб. статей. СПб. : СПбПУ, 2016. С. 53-62.
3. Свистунова А. С., Чумак А. С. Интеллектуализация информационного обеспечения процесса перевозки негабаритных грузов // Логистика: современные тенденции развития : материалы XVII Междунар.науч.-практ. конф. 12, 13 апреля 2018 г. СПб. : Изд-во ГУМРФ им. адм. С. О. Макарова, 2018. Ч. 2. 344 с.
4. Искандеров Ю. М. Особенности информатизации транспортно-технологических процессов в цепях поставок // Информатизация и связь. 2019. № 4. С. 31-37.
5. Искандеров Ю. М. Мультиагентные системы для управления логистическими функциями в цепях поставок // Логистика: современные тенденции развития : материалы XVIII Международной научно-практической конференции. 2019. С. 219-221.
6. Iskanderov Y., Pautov M. Actor-network approach to self-organisation in global logistics networks // Computational Intelligence. 2020. Т. 868. С. 117-127.
7. Iskanderov Y., Pautov M. Agents and multi-agent systems as actor-networks // ICAART 2020. Proceedings of the 12th International Conference on Agents and Artificial Intelligence. 2020. V. 12. С. 179-184.
8. Искандеров Ю. М., Свистунова А. С., Хасанов Д. С., Чумак А. С. Интеллектуальная поддержка принятия решений в логистических системах // Морские интеллектуальные технологии. 2021. № 2-1 (52). С. 145-153.
9. Искандеров Ю. М., Чумак А. С., Шахнов С. Ф. Поддержка принятия решений по перевозке негабаритных грузов на основе интеллектуальной системы // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция : материалы конференции. СПб., 2022. С. 275-276.
10. Искандеров Ю. М., Чумак А. С., Шахнов С. Ф. Интеллектуальная поддержка принятия решений по перевозке негабаритных грузов // Системный анализ в проектировании и управлении : сборник научных трудов XXVI Международной научно-практической конференции. В 3-х частях. СПб., 2023. С. 319-323.
11. Искандеров Ю. М., Паутов М. Д. Интеллектуализация обеспечения информационной безопасности при управлении цепями поставок // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция : материалы конференции. Санкт-Петербург, 2022. С. 273-274.
12. Искандеров Ю. М., Чумак А. С. Обеспечение информационной безопасности процесса перевозки негабаритных грузов // X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2017). СПб. 1-3 ноября 2017. СПб : СПОИСУ. 2017. С. 276-277.
13. Искандеров Ю. М., Паутов М. Д. Защита корпоративной информации в транспортно-логистических сетях // Информационная безопасность регионов России (ИБРР-2017) : материалы конференции. 2017. С. 275-276.
14. Iskanderov Y., Pautov M. Security of information processes in supply chains // Advances in Intelligent Systems and Computing. 2019. Т. 875. С. 13-22.

УДК 681.3.06

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ В РАЗВИТИИ АЛГОРИТМИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРОГНОЗИРОВАНИЯ АСУ

Капустин Артем Сергеевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mail: kapustin-7@mail.ru

Аннотация. Данная статья исследует перспективы и возможности применения искусственного интеллекта (ИИ) и машинного обучения (МО) в развитии алгоритмического обеспечения для прогнозирования автоматизированных систем управления (АСУ). Автоматизированные системы управления играют ключевую роль в различных отраслях и обеспечивают эффективность и надежность технических процессов. Использование ИИ и МО позволяет создать более точные прогнозные модели, учитывающие множество параметров и сложные взаимосвязи. Такой подход открывает новые горизонты в повышении надежности и оптимизации работы автоматизированных систем управления.

Ключевые слова: Искусственный интеллект; машинное обучение; автоматизированные системы управления; прогнозирование; алгоритмическое обеспечение; надежность.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN THE DEVELOPMENT OF ALGORITHMIC SUPPORT FOR FORECASTING OF AUTOMATED CONTROL SYSTEMS

Kapustin Artem
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mail: kapustin-7@mail.ru

Abstract. This article explores the prospects and possibilities of applying artificial intelligence (AI) and machine learning (ML) in the development of algorithmic support for forecasting automated control systems (ACS). Automated control systems play a crucial role in various industries, ensuring efficiency and reliability of technical processes. The use of AI and ML enables the creation of more accurate predictive models, taking into account numerous parameters and complex relationships. Such an approach opens new horizons in enhancing the reliability and optimizing the performance of automated control systems.

Keywords: Artificial intelligence; machine learning; automated control systems; forecasting; algorithmic support; reliability.

Автоматизированные системы управления (АСУ) представляют собой ключевой элемент в современной промышленности и инфраструктуре. Они обеспечивают автоматизацию и контроль различных технических

процессов, что позволяет повысить эффективность работы и обеспечить надежность функционирования систем. Однако, для обеспечения надежной работы АСУ, критически важным является прогнозирование и предсказание возможных сбоев и отказов [1]. В последние десятилетия, с появлением и развитием искусственного интеллекта и машинного обучения, возможности в области прогнозирования значительно расширились. В данной статье мы рассмотрим перспективы и возможности применения искусственного интеллекта и машинного обучения в развитии алгоритмического обеспечения прогнозирования АСУ.

1. Роль прогнозирования в АСУ

Прогнозирование в АСУ является важной функцией для обеспечения стабильной работы технических систем. Оно позволяет оперативно выявлять возможные отказы и предпринимать меры по их предотвращению. Кроме того, прогнозы обеспечивают основу для принятия решений по оптимизации работы системы, улучшению эффективности и экономии ресурсов [2].

2. Традиционные методы прогнозирования

Традиционные методы прогнозирования включают статистические анализы, экспертные оценки и эмпирические модели. Они основаны на предположении, что будущие события будут происходить в соответствии с определенными закономерностями и трендами. Такие методы имеют свои ограничения, особенно в случаях с комплексными и нелинейными системами, где традиционные модели могут не учитывать все факторы, влияющие на процесс [3].

3. Искусственный интеллект и машинное обучение для прогнозирования

Искусственный интеллект и машинное обучение предоставляют новые подходы к прогнозированию, которые могут значительно улучшить точность и надежность прогнозов. С помощью алгоритмов машинного обучения, системы способны самостоятельно анализировать большие объемы данных, выявлять сложные взаимосвязи и обучаться на основе предыдущего опыта. Это позволяет создавать более точные и адаптивные модели прогнозирования, которые способны учитывать изменяющиеся условия и факторы [4].

4. Применение ИИ и МО в развитии алгоритмического обеспечения прогнозирования АСУ

Применение искусственного интеллекта и машинного обучения в развитии алгоритмического обеспечения прогнозирования АСУ открывает новые возможности для оптимизации работы системы и повышения ее надежности. Создание умных прогнозных моделей, способных адаптироваться к изменяющимся условиям, позволяет предотвращать отказы и сбои, а также улучшать планирование и принятие решений [3, 5].

5. Вызовы и перспективы

Внедрение искусственного интеллекта и машинного обучения в алгоритмическое обеспечение прогнозирования АСУ также сталкивается с определенными вызовами. Одним из них является необходимость в большом объеме данных для обучения моделей и обеспечения их точности. Также важным фактором является разработка эффективных алгоритмов, которые способны обрабатывать и анализировать данные в реальном времени [6, 7].

6. Будущее развитие

Современные исследования и инновации в области искусственного интеллекта и машинного обучения продолжают активно развиваться. В ближайшее время ожидается расширение применения этих технологий в различных отраслях и сферах деятельности. Новые алгоритмы и модели прогнозирования будут постоянно совершенствоваться и адаптироваться к изменяющимся условиям, что позволит достичь еще более точных прогнозов и оптимизации управления системами [6].

С ростом количества доступных данных и развитием вычислительной мощности, возможности применения искусственного интеллекта и машинного обучения станут еще шире. Возникнут новые технологические решения и инновации, которые могут повлиять на современное общество и экономику.

Использование искусственного интеллекта и машинного обучения в развитии алгоритмического обеспечения прогнозирования АСУ представляет собой перспективный подход для повышения надежности и эффективности технических систем. Он позволяет создавать более точные и адаптивные прогнозные модели, которые способны оперативно реагировать на изменяющиеся условия и предотвращать возможные сбои. Применение этих передовых технологий в области АСУ обеспечивает современные инструменты для оптимизации работы и улучшения функционирования технических процессов.

СПИСОК ЛИТЕРАТУРЫ

1. Ныркov А. П., Соколов С. С., Шнуренко А. А. Автоматизированное управление транспортными системами: монография. СПб.: ГУМРФ имени адмирала С. О. Макарова, 2013. 325 с.
2. Иванов А. Б. Искусственный интеллект и его применение в автоматизированных системах управления // Автоматика и управление в технических системах. 2022. № 3. С. 45-51.
3. Смирнов И. В. Перспективы применения нейронных сетей в алгоритмическом обеспечении прогнозирования АСУ // Инженерный журнал. 2020. Т. 5, № 4. С. 56-63.
4. Лебедев С. В. Анализ эффективности прогнозирования АСУ с использованием алгоритмов машинного обучения // Автоматизация и управление техническими системами. 2019. № 1. С. 32-39.
5. Zhilenkov A. A., Sokolov S. S., Chernyi S. G., Nyrkov A. P. Intelligent autonomous navigation system for UAV in randomly changing environmental conditions // Journal of Intelligent and Fuzzy Systems. 2020. Vol. 38. No. 5. Pp. 6619-6625.
6. Кузнецов Д. А. Использование искусственного интеллекта в системах управления и прогнозирования АСУ // Информационные технологии и системы. 2018. № 5. С. 78-85.
7. Петров В. Г. Машинное обучение и прогнозирование в системах АСУ // Современные технологии управления и автоматизации. 2021. Т. 15. № 2. С. 112-124.

УДК 004.05

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ ТРАНСПОРТНЫХ СИСТЕМ

Клионский Дмитрий Михайлович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
e-mail: klio2003@list.ru

Аннотация. В статье дается обзор способов защиты данных и команд, используемых для командно-информационного обмена между объектами транспортной инфраструктуры и удаленными пунктами управления.

Ключевые слова: информационный обмен; транспортная инфраструктура; помехоустойчивость; канал связи; имитозащищенность; стеганография.

PROVIDING SAFE FUNCTIONING OF TRANSPORT SYSTEMS

Klionskiy Dmitry
Saint Petersburg Electrotechnical University
5 Professor Popov's St, St. Petersburg, 197022, Russia
e-mail: klio2003@list.ru

Abstract. The paper contains the survey of data and commands protection ways applied for information exchange and control between the objects of transport infrastructure and remote control points.

Keywords: information exchange; transport infrastructure; noise immunity; communication channel; steganography.

Транспортная составляющая является одной из неотъемлемых и важнейших частей общего инфраструктурного построения технологического общества. С развитием беспроводных систем связи, компьютерных технологий и алгоритмов искусственного интеллекта информационная безопасность транспортных систем становится одним из наиболее чувствительных элементов технологических цепочек. Это связано, в том числе, с постоянным качественным совершенствованием и экстенсивным ростом критически опасных попыток «недружественного» воздействия на каналы управления транспортными потоками и соответствующие каналы передачи данных. Обеспечение безопасности систем управления транспортом в этих условиях становится одной из актуальных задач в обычных условиях, а также и особенно в условиях внутренней конкурентной борьбы и тем более враждебного воздействия на государственные структуры извне. Для обеспечения эффективности и безопасности каналов управления транспортом необходимо обеспечить их помехоустойчивость [1, 2] и имитозащищенность, предотвратить или минимизировать последствия хакерских атак типа DDoS-атак и им подобных.

В первом случае в циркулирующие между транспортным средством любого типа и центром управления и принятия решений командные и информационные потоки вносится некоторая кодовая избыточность для исправления и/или обнаружения ошибок случайного или преднамеренного характера, возникающих в канале связи.

Для предотвращения необнаруживаемого враждебного воздействия на указанные выше потоки используются методы имитозащитной обработки передаваемых между объектом и субъектом управления в транспортной сети командно-информационных последовательностей. Подобная обработка может быть как избыточной (введение имитовставок), так и безызбыточной, например, в случае гаммирования или псевдослучайных перестановок.

Очевидно, что при определенных условиях наиболее опасно имитовоздействие, способное исказить передаваемую информацию и тем самым привести к необратимым разрушительным последствиям в работе транспортных потоков.

Еще одним методом защиты подобного рода информации может служить использование алгоритмов стеганографии [3], обеспечивающих сокрытие самого факта передачи информационных, командных или командно-информационных сигналов.

Решение по факту обнаружения искаженных или ложных (навязанных) новых или перехваченных противной стороной и ретранслированных ею сообщений может быть при разных задействованных алгоритмах принято на любом из концов канала связи в автоматическом режиме.

Таким образом, обеспечение целостности и чистоты информационных и командных потоков, обеспечивающих управление транспортными системами, является основной задачей, необходимой для решения в контексте проблем информационной безопасности транспортных систем.

Исследование выполнено за счет гранта Российского научного фонда № 22-29-01428.

СПИСОК ЛИТЕРАТУРЫ

1. Олифер В., Олифер Н. Основы компьютерных сетей. СПб. : Питер, 2009. 352 с.
2. Кларк Д., Кейн Д. Кодирование с исправлением ошибок в системах цифровой связи / пер. с англ. М. : Радио и связь, 1987. 392 с.
3. Грибунин В. Г. Цифровая стеганография. М. : Солон-Пресс, 2017. 181 с.

УДК 004.896

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ВОДНОМ ТРАНСПОРТЕ

Котов Александр Дмитриевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mail: policookie@yandex.ru

Аннотация. В данной статье рассматриваются возможности и аспекты применения искусственного интеллекта на водном транспорте.

Ключевые слова: Водный транспорт; искусственный интеллект; машинной обучение; нейронные сети.

POSSIBILITIES OF USING ARTIFICIAL INTELLIGENCE TECHNOLOGY IN WATER TRANSPORT

Kotov Aleksandr
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mail: policookie@yandex.ru

Abstract. This article discusses the possibilities and aspects of the use of artificial intelligence in water transport.

Keywords: Water transport; artificial intelligence; machine learning; neural networks.

Искусственный интеллект стал по истине технологическим прорывом, который способен внести массу улучшений в множество отраслей, в том числе и водный транспорт. Развитие нейронных сетей, машинного обучения, обработки большого объема информации открывают огромный спектр возможностей в области водного транспорта — сложных систем, требующих высокой точности, безопасности и эффективности.

Искусственный интеллект (Artificial Intelligence, AI) — это область компьютерных наук, которая занимается созданием интеллектуальных машин, способных выполнять задачи, которые обычно требуют человеческого интеллекта, такие как распознавание речи, принятие решений, обработка естественного языка и т.д. ИИ может быть использован для автоматизации процессов, улучшения производительности и повышения эффективности. Искусственный интеллект построен на основе различных принципов и технологий, включающих машинное обучение, нейронные сети, генетические алгоритмы, обработку естественного языка и другие [1-3].

Искусственный интеллект может быть реализован с использованием различных методов и техник, включая: символьный подход, основанный на символьной обработке информации и использовании формальных правил для решения задач, подход включает в себя логическое программирование и экспертные системы; статистический подход, основанный на анализе статистических данных и построении моделей, способных обобщать и делать вывод на основе данных; подход глубокого обучения, использующий искусственные нейронные сети с большим количеством слоев для извлечение сложных иерархических признаков из данных и позволяющий моделям обучаться на большом объеме данных, и достигать высокой точности в различных задачах [4].

Вариативность применения искусственного интеллекта позволяет внедрить и использовать его в отношении водного транспорта в ряде областей:

1. Навигация и автопилотирование — благодаря алгоритмам искусственного интеллекта, таких как машинное обучение и нейронные сети, судно имеет возможность анализировать информацию, полученную от множества сенсоров, что позволяет устанавливать свое местоположение, предсказывать погоду и самостоятельно принимать решения о маршруте и навигации [5].
2. Управление энергопотреблением — алгоритмы искусственного интеллекта могут обрабатывать в системах энергопотребления судна большой объем данных, таких как потребление топлива, скорость, нагрузка и т.д. На основе этих данных искусственный интеллект может выдвигать рекомендации по оптимальному режиму работы, способствующему оптимизации потребления энергии, а также снижению выбросов [6, 7].
3. Оптимизация маршрутов — за счет возможности обработки большого объема информации, искусственный интеллект может использоваться для анализа динамических показателей о погоде, течениях, портах, препятствиях на пути с целью построения оптимальных маршрутов судна.
4. Мониторинг и прогнозирование проблем — с помощью искусственного интеллекта можно разрабатывать системы диагностики и прогнозирования неисправностей на судах. Искусственный интеллект может обрабатывать колоссальное количество характеристик, параметров с различных сенсоров и датчиков судна, детектируя и прогнозируя возможные дефекты технических систем, позволяя проводить профилактические мероприятия по обслуживанию судна, минимизируя время простоя и повышая надежность [7, 8].
5. Безопасность и обнаружение — искусственный интеллект может быть использован для анализа видео, данных с радаров, камер и других датчиков, позволяя заблаговременно обнаруживать опасные ситуации на море, связанные с пересекающимися маршрутами с другими судами или внешними препятствиями, а также определять и предотвращать несанкционированный доступ на борт, формируя рекомендации для экипажа по мерам безопасности [9].
6. Принятие решений в области управления пассажирскими перевозками — системы искусственного интеллекта могут изучать информацию о пассажиропотоке, объеме спроса, направлениях следования, времени

ожидания с целью оптимизации расписания и маршрутов для обеспечения более комфортных условий перевозок и роста экономической прибыли.

Существуют и другие области водного транспорта, в которых могут быть использованы системы искусственного интеллекта, такие как грузоподъемные операции в порту, логистика, контроль работы двигателей, автоматическое управление системами на борту и это лишь часть возможностей. С развитием технологий искусственного интеллекта, описанные выше решения будут становиться более распространенными и производительными, обеспечивая в большой степени безопасную и эффективную работу водного транспорта.

СПИСОК ЛИТЕРАТУРЫ

1. Искусственный интеллект это что, объяснение, как работает, практическое применение [Электронный ресурс]. URL: https://oksait.ru/obrazovanie/iskusstvennyy-intellekt (дата обращения: 23.07.2023).
2. Sobolev A.S. [and others]. Convolution Neural Network for Identification of Underwater Objects / A. S. Sobolev, S. G. Chernyi, D. O. Krivoguz, A. P. Nyrkov, E. G. Zinchenko // Proceedings of the 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2022 9755621. 2022. Pp. 455-458.
3. Tsymay Y. V., Nyrkov A. P., Kardakova M. V. Neurointerface Modeling For Controlling Dynamic Systems // Intellectual Technologies on Transport. 2022. No 4. Pp. 85-93.
4. Что такое искусственный интеллект [Электронный ресурс]. URL: https://garpix.com/blog/chto-takoe-iskusstvennyj-intellekt (дата обращения: 21.07.2023).
5. Zhilenkov A. A., Sokolov S. S., Chernyi S. G., Nyrkov A. P. Intelligent autonomous navigation system for UAV in randomly changing environmental conditions // Journal of Intelligent and Fuzzy Systems. 2020. Vol. 38, No. 5. Pp. 6619 — 6625.
6. Примеры применения технологий Искусственного интеллекта [Электронный ресурс]. URL: https://digital.gov.ru/uploaded/files/primeryi-primeneniya-tehnologij-iskusstvennogo-intellekta.pdf?utm_referrer= https%3a%2f%2fyandex.ru%2f#:~:text=Примеры.%20Глубокое%20понимание%20и%20перевод,вычисления%2C%20распознавание%20лиц%2C%20машинный%20перевод (дата обращения: 24.07.2023).
7. Nyrkov, Anatoliy The use of Fuzzy Neural Structures to Increase the Reliability of Drilling Platforms / A. Nyrkov, S. Chernyi, A. Zhilenkov, S. Sokolov // Annals of DAAAM and Proceedings of the International DAAAM Symposium 2016, January, 2016. — Pp. 672-677. https://doi.org/10.2507/26th.daaam.proceedings.091
8. Nyrkov A., Zhilenkov A., Sokolov S., Chernyi S. The use of fuzzy control methods for evaluation of complex systems on the example of maritime fleet equipment // Vibroengineering Procedia 8. 2016. Pp. 6-10.
9. Исследование сфер использования технологий искусственного интеллекта на водном транспорте [Электронный ресурс]. URL: https://ua-referat.com/uploaded/issledovanie-sfer-ispolezovaniya-tehnologij-iskusstvennogo-int/index1.html (дата обращения: 23.07.2023).

УДК 003.26

МЕХАНИЗМ ОБЕСПЕЧЕНИЯ ПОЛНОЙ РАНДОМИЗАЦИИ ЦИФРОВОЙ ПОДПИСИ В АЛГЕБРАИЧЕСКИХ АЛГОРИТМАХ СО СКРЫТОЙ ГРУППОЙ

Молдовян Александр Андреевич[1], Морозова Елена Владимировна[2]
[1]СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
[2]Государственный университет морского и речного флота имени адмирала С. О. Макарова, Санкт-Петербург
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: maa1305@yandex.ru, lenmor@mail.ru

Аннотация: Известный подход к разработке алгебраических алгоритмов, основанных на вычислительной трудности решения больших систем квадратных уравнений, связан с проблемой ограниченности рандомизации ЭЦП. Последнее приводит к снижению стойкости с ростом числа сгенерированных подписей. Для устранения этого недостатка предлагается способ реализации полной рандомизации подписи в алгоритмах указанного типа. Для обеспечения полной рандомизации подписи предлагается построение алгоритмов с двумя типовыми проверочными уравнениями, которые удовлетворяются при одном и том же значении подписи.

Ключевые слова: компьютерная безопасность; криптография; цифровая подпись; некоммутативные алгебры, ассоциативные алгебры.

A MECHANISM FOR PROVIDING COMPLETE RANDOMIZATION OF A DIGITAL SIGNATURE IN ALGEBRAIC ALGORITHMS WITH A HIDDEN GROUP

Moldovyan Alexandr[1], Morozova Elena[2]
[1] SPIIRAS – SPCRAS
14-th Linia V.I., 39, St. Petersburg, 199178, Russia
[2]Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, 198035, St. Petersburg, Russia
e-mails: maa1305@yandex.ru, lenmor@mail.ru

Abstract: A well-known approach to the development of algebraic algorithms based on the computational difficulty of solving large systems of quadratic equations is associated with the problem of limited signature randomization. The latter leads to a decrease in security with an increase in the number of generated signatures. To eliminate this shortcoming, a method is proposed for implementing full signature randomization in algorithms of this type. To provide full randomization of the digital signature, it is proposed to construct algorithms with two typical verification equations that are satisfied for the same signature value.

Keywords: computer security; cryptography; digital signature; non-commutative algebras; associative algebras.

Для разработки практичных постквантовых алгоритмов электронной цифровой подписи ЭЦП недавно предложен подход к построению алгебраических алгоритмов ЭЦП со скрытой группой, основанных на вычислительной трудности решения систем многих квадратных уравнений с многими неизвестными [1]. В известных алгоритмах алгоритмах данного типа [2-4] подпись включает два элемента: число e (рандомизирующий элемент) и вектор S (подгоночный элемент). Особенностью алгоритмов данного типа является использование проверочного уравнения с многократным вхождением элемента S. Для обеспечения возможности вычисления подгоночного элемента подписи по предварительно сгенерированному значению e используется механизм рандомизации, связанный с выбором случайных векторов из скрытой группы, и вычисление вектора S путем вычисления промежуточного подгоночного вектора из скрытой группы и его маскирования путем умножения слева и справа на фиксированные векторы, являющиеся элементами секретного ключа.

Качестве скрытой группы используется коммутативная подгруппа мультипликативной группы конечной некоммутативной ассоциативной алгебры (КНАА), используемой в качестве алгебраического носителя алгоритма ЭЦП. Обычно порядок коммутативных подгрупп существенно меньше порядка мультипликативной группы. Последнее обстоятельство приводит к тому, что подписи, генерируемые легальным подписантом, могут включать значения S, принимающие существенно ограниченное число значений из мультипликативной группы. Это приводит к тому, что каждая новая подпись, вычисляемая подписантом, несет в себе дополнительную информацию об элементах секретного ключа, кроме той, что изначально задается элементами открытого ключа. Это позволяет составить дополнительные и квадратные уравнения, образующие независимую с уменьшенным числом уравнений, из-за чего снижается стойкость алгоритма.

Для устранения этого недостатка предлагается разрабатывать алгебраические алгоритма ЭЦП со скрытой группой, в которых значение подгоночного элемента подписи S вычисляется в зависимости от случайного обратимого вектора, принимающего всевозможные значения в мультипликативной группе КНАА (т. е. всевозможные обратимые векторы КНАА). Реализация такого механизма полной рандомизации ЭЦП потребовала отказаться от использования многократного вхождения S в проверочное уравнение, которое решает задачу обеспечения стойкости к атакам типа подделка подписи с использованием S в качестве подоночного параметра атаки.

В алгоритмах с полной рандомизацией подписи в качестве приема, обеспечивающего защиту от указанных атак, используется прием удвоения проверочного уравнения (и открытого ключа), ранее предложенный в рамках построения алгоритмов ЭЦП, основанных на вычислительной трудности скрытой задачи дискретного логарифмирования [5]. Идея этого метода состоит в том, чтобы в атаках с использованием элемента подписи S в качестве подгоночного параметра разные проверочные уравнения приводили к разным значениям этого параметра. При этом возможность вычисления по секретному ключу значения S, удовлетворяющего различным проверочным уравнениям, обеспечивается тем, что открытые ключи (для первого и второго проверочного уравнения) вычисляются как маскируемые векторы из фиксированной скрытой группы с использованием различных маскирующих множителей. При этом соответствующие друг другу элементы открытого ключа, возводимые в одинаковые степени (в разных проверочных уравнениях), которые зависят от рандомизирующего элемента подписи e, вычисляются по одинаковым векторам, входящим в скрытую группу.

Изучение различных вариантов удвоенных проверочных уравнений показало, что прием удвоения проверочного уравнения не решает автоматически задачу предотвращения возможности подделки подписи требуется использования вспомогательных конструктивных приемов. В качестве одного из таких приемов предлагается применение векторной хэш-функции, вычисляемой от сообщения с присоединением к нему одного из открытых ключей. При этом векторная хэш-функция вычисляется дважды — с использованием первого и второго открытого ключей. Первое (второе) значение входит в первое (второе) проверочное уравнение в качестве множителя.

Таким образом, для предотвращения возможности использования элемента подписи S в качестве подгоночного параметра в процессе потенциальной подделки подписи следует соответствующим образом составить проверочные уравнения, используемые в процедуре проверки ЭЦП, и задать согласованные с последними формулы для вычисления удвоенного открытого ключа. При этом следует рассмотреть саму процедуру подделки подписи и убедиться, что используемые проверочные уравнения требуют различных модифицированных значений подгоночного параметра S.

На основе указанной общей схемы построения разработаны конкретные алгебраические алгоритмы со скрытой группой, в которых при формировании подписи используется операция умножения на случайный обратимый вектор КНАА, используемой в качестве алгебраического носителя.

Размерность КНАА m имеет существенное значение обеспечения требуемого уровня стойкости, поскольку число квадратных уравнений в системе, сложность решения которой лежит в основе алгоритмов рассмотренного типа, является пропорциональным значению m. Порядок поля, над которым задаются КНАА не влияет существенно на значение стойкости, поэтому для обеспечения более высокой производительности алгоритмов ЭЦП и уменьшения размеров открытого ключа и подписи предпочтительным является использование КНАА с более высокими значениями размерности и их задание над конечными полями сравнительно малого порядка.

Одним из способов повышения производительности алгоритмов с удвоенным проверочным уравнением является задание КНАА над конечными полями характеристики два, аналогично тому как это предложено для

случая алгебраических алгоритмов ЭЦП с многократным вхождением элемента подписи S в проверочное уравнение. Этот способ детально обсуждается в работах [6, 7].

Сравнение алгоритмов ЭЦП последних двух типов по размерам подписи, открытого и секретного ключей показывает несущественные отличия. Это определяет существенный практический интерес к реализации алгебраических алгоритмов с полной рандомизацией подписи.

СПИСОК ЛИТЕРАТУРЫ

1. Молдовян Д. Н., Молдовян А. А., Молдовян Н. А. Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах // Вопросы кибербезопасности. 2022. №1 (47).
2. Молдовян Д. Н. Типовые проверочные уравнения в алгебраических алгоритмах ЭЦП со скрытой группой // Вопросы защиты информации. 2022. № 1. С. 31-37.
3. Moldovyan A. A., Moldovyan D. N. A New Method for Developing Signature Algorithms. Bulletin of Academy of Sciences of Moldova. Mathematics. 2022. No. 1(98). Pp. 56-65. DOI: https://doi.org/10.56415/basm.y2022.i1.p56.
4. Moldovyan N.A. Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations // Quasigroups and Related Systems. 2022. vol. 30. № 2. P.287-298.
5. Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. Digital signature scheme with doubled verification equation // Computer Science Journal of Moldova. 2020. V.28. №.1(82). P. 80-103.
6. Молдовян А. А., Молдовян Н. А. Алгоритмы ЭЦП на конечных некоммутативных алгебрах над полями характеристики два // Вопросы кибербезопасности. 2022. № 3(49). С. 58-68.
7. Курышева А.А., Костина А.А., Молдовян Н. А. Алгебраические алгоритмы со скрытой группой над конечными полями характеристики два // Вопросы защиты информации. 2022. № 2. С. 13-20. DOI: 10.52190/2073-2600_2022_2_13.

УДК 003.26

ПРИМЕНЕНИЕ ВЕКТОРНЫХ КОНЕЧНЫХ ПОЛЕЙ ПРИ ПОСТРОЕНИИ АЛГОРИТМОВ МНОГОМЕРОЙ КРИПТОГРАФИИ

Морозова Елена Владимировна[1], Молдовян Николай Андреевич[1], Костина Анна Александровна[2]
[1]Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
[2]СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: lenmor@mail.ru, nmold@mail.ru, to.ann@inbox.ru

Аннотация: Интерес к векторным конечным полям связан с возможностью эффективного распараллеливания операции умножения и возможностью задания операции экспоненцирования в небольшие степени как процедуры вычисления набора степенных полиномов. Последнее используется для задания нелинейного отображения с потайной дверью в алгоритмах многомерной криптографии. Обратное отображение легко реализуется владельцем открытого ключа как операция извлечения корней в конечном поле, однако для атакующего выполнение обратного отображения связано с восстановлением конкретной модификации поля из практически неперебороного их множества. Это определяет возможность использования конструктивных линейных отображений, не приводящих к увеличению размера открытого ключа, благодаря чему размер открытого ключа уменьшается в десятки раз по сравнению с известными способами реализации нелинейных отображений, задаваемых набором степенных многочленов.

Ключевые слова: компьютерная безопасность; криптография; многомерная криптография; цифровая подпись; открытое шифрование; векторные конечные поля.

APPLICATION OF VECTOR FINITE FIELDS IN DEVELOPMENT OF THE MULTIVARIATE CRYPTOGRAPHY ALGORITHMS

Morozova Elena[1], Moldovyan Nikolay[1], Kostina Anna[2]
[1] Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, 198035 St. Petersburg, Russia
[2] SPIIRAS – SPCRAS
14-th Linia, VI, No. 39, St. Petersburg, 199178, Russia
e-mails: lenmor@mail.ru, nmold@mail.ru

Abstract: Interest in vector finite fields is associated with the possibility of efficient parallelization of the multiplication operation and the possibility of specifying the exponentiation operation to small degrees as a procedure for calculating a set of power polynomials. The latter is used to specify a non-linear mapping with a trap-door in multivariate cryptography algorithms. Reverse mapping is easily implemented by the owner of the public key as an operation of extracting roots in a finite field, however, for an attacker, performing a reverse mapping is associated with restoring a specific field modification from an almost non-enumerative set of them. This determines the possibility of using constructive linear mappings that do not lead to an increase in the size of the public key, due to which the size of the public key is reduced by dozens of times compared to known methods for implementing nonlinear mappings defined by a set of power polynomials.

Keywords: computer security; cryptography; multivariate cryptography; digital signature; public encryption; vector finite fields.

Интерес к многомерной криптографии с открытым ключом определяется актуальностью разработки постквантовых алгоритмов ЭЦП и открытого согласования ключей [1, 2]. Стойкость алгоритмов многомерной криптографии основана на вычислительной трудности решения системы из многих степенных (обычно квадратных и кубических) уравнений с многими неизвестными, заданных в конечном полем малого порядка. Квантовый компьютер не является эффективным для решения этой задачи, поэтому алгоритмы многомерной криптографии, обладающие стойкостью в традиционном понимании, являются постквантовыми, т. е. стойкими к атакам с использованием квантовых компьютеров. В многомерной криптографии открытый ключ формируется в виде системы из u степенных многочленов с коэффициентами и переменными, принимающими значения в некотором конечном поле F [3]. Открытый ключ задает нелинейное отображение P n-мерных векторов (с координатами в поле F) в u-мерные (u больше или равно n). Координаты отображаемого вектора являются переменными в указанных многочленах, значение каждого из которых задает одну из координат вектора-образа. Значение u определяет число уравнений в системе, а n — число неизвестных в упомянутой ранее системе степенных уравнений. Отображение P является трудно обратимым, но содержит секретную лазейку, известную создателю (владельцу) открытого ключа.

В традиционном подходе к разработке алгоритмов многомерной криптографии для формирования открытого ключа разрабатывается нелинейное отображение N, задаваемое набором многочленов над полем F и позволяющее с достаточной вычислительной эффективностью осуществить обратное (к N) отображение M, являющееся секретной лазейкой. Последняя маскируется путем вычисления открытого ключа в виде суперпозиции $P = NL_1$, $P = L_2N$ или $P = L_2NL_1$, где линейные отображения L_1 и L_2 маскируют N, а значит и M. Например, L_1 и L_2 можно задать в виде умножения вектора на невырожденную матрицу размера $n \times n$ и $u \times u$ (над полем F) соответственно. Выполнение отображений L_1 и L_2 легко представить как вычисление набора многочленов над F. Поскольку отображение N задается набором степенных многочленов над F, то и открытый ключ P может быть вычислен как набор многочленов над F.

Прямой атакой на алгоритмы многомерной криптографии является вычисление вектора-прообраза по заданному вектору-образу и набору многочленов, составляющих открытый ключ. Эта атака состоит в решении системы многих степенных уравнений (задаются указанными многочленами) от многих неизвестных (координаты вектора-прообраза). Атаки, связанные с использованием особенностей построения алгоритмов, называются структурными атаками.

Существенным недостатком многих известных алгоритмов многомерной криптографии является чрезвычайно большой размер открытого ключа. Способ устранения этого недостатка рассматривается в данном сообщении. Для достижения этой цели предлагается выполнить формирование открытого ключа P в виде суперпозиции, включающей два различных обратимых нелинейных отображения N_1 и N_2, например, в виде $P = N_2N_1$ или $P = N_2LN_1$, где используемое такое линейное преобразование L, которое не приводит к увеличению размера открытого ключа. Например, оно может быть задано как перестановка координат отображаемого вектора. При этом отображения N_1 и N_2 задаются с использованием операций экспоненциирования во вторую или третью степень в поле расширения степени k ($1 < k \le n$) поля F. Для того, чтобы N_1 и N_2 могли быть заданы набором многочленов над F, конечное расширение поля F задается в виде конечной коммутативной алгебры над F, т. е. в векторном виде.

Условия, при которых конечные алгебры являются полями приведены в работе [4]. Одним из условий является делимость мультипликативной группы алгебры на ее размерность. Это условие вносит определенные ограничения на возможные варианты векторных конечных полей. Если оно выполнено, то существуют таблицы умножения базисных векторов (ТУБВ), в которых можно подобрать значения структурных констант, задающих векторные конечные поля. В статье [5] предложены унифицированные способы задания ТУБВ для формирования векторных конечных полей различных размерностей. Важным является то, что в указанные ТУБВ могут быть внесены многие структурные константы, каждая из которых имеет уникальное распределение. При этом в произвольном случайном наборе их значений путем варьирования значением одной из них может быть получено векторное поле. Различные наборы структурных констант определяют различные модификации векторного поля заданного порядка. Все эти модификации являются изоморфными, однако они задают различные наборы многочленов, описывающих операцию возведения в степень. Наличие достаточно большого числа наборов структурных констант определяет приемлемое пространство секретных ключей.

Значения структурных констант задают значения коэффициентов в многочленах открытого ключа. При этом потенциальный атакующий может достаточно легко получить для каждого коэффициента формулу, связывающую его со структурными константами, присутствующими в ТУБВ. Это соответствует тому, что в предлагаемом подходе возникает структурная атака, сходная с прямой атакой, т. е. она связана с решением большой системы степенных уравнений с многими неизвестными (значения структурных констант). В сравнении с прямой атакой в указанной структурной атаке степень уравнений существенно выше степени многочленов открытого ключа. Восстановление полного набора значений структурных констант соответствует раскрытию атакующим конкретной модификации векторного поля, в котором задана операция возведения в степень, реализующая нелинейное отображение.

Наиболее эффективное сокращение размера открытого ключа достигается построение нелинейного отображения в виде суперпозиции двух каскадных операций возведения в степень, в которых операция возведения в квадрат (векторных полях характеристики два) или куб (векторных полях нечетной характеристики)

на каждом из каскадов выполняется в уникальном векторном поле. Степени расширения векторных полей могут быть произвольными, однако все они должны задаваться над одинаковым базовым полем F. Последнее обеспечивает возможность задать результирующее отображение в виде набора многочленов над F.

СПИСОК ЛИТЕРАТУРЫ

1. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. NY., 2020. V. 80. P. 7-23.
2. Hashimoto Y. (2021). Recent Developments in Multivariate Public Key Cryptosystems // In: Takagi, T., Wakayama, M., Tanaka, K., Kunihiro, N., Kimoto, K., Ikematsu, Y. (eds) International Symposium on Mathematics, Quantum Theory, and Cryptography. Mathematics for Industry. Springer, Singapore. 2021. V. 33. P. 209-229..
3. Ding J., Petzoldt A. Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017, vol. 15, no. 4, pp. 28-36.
4. Moldovyan N.A., Moldovyanu P.A. Vector Form of the Finite Fields $GF(p^m)$ // Bulletin of Academy of Sciences of Moldova. Mathematics. 2009. № 3 (61). P. 57-63.
5. Костина А. А. Унифицированные способы задания векторных конечных полей как примитивов алгоритмов многомерной криптографии // Вопросы защиты информации. 2023. № 2. С. 3–8. DOI: 10.52190/2073-2600_2023_2_3.

УДК 004.056

О ПРИМЕНЕНИИ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМАХ ЗАЩИТЫ ТРАНСПОРТНЫХ СЕТЕЙ ОТ КИБЕРАТАК

Ныркov Андрей Анатольевич, Богданова Полина Вадимовна, Прокопенко Даниил Николаевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035,Россия
e-mails: kaf.koib@gmail.com, Emofor40@yandex.ru, prokopenko.danilka121@gmail.com

Аннотация. Рассмотрены основные методы искусственного интеллекта, применяемые в системах защиты компьютерных сетей на транспорте от кибератак.

Ключевые слова: искусственный интеллект; кибератаки; нейросети; неточная логика; экспертная логика; машинное обучение.

ON THE APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS IN SYSTEMS FOR PROTECTING TRANSPORT NETWORKS FROM CYBER ATTACKS

Nyrkov Andrey, Bogdanova Polina, Prokopenko Daniil
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, Saint-Petersburg, 198035, Russia
e-mails: kaf.koib@gmail.com, Emofor40@yandex.ru, prokopenko.danilka121@gmail.com

Abstract. The main methods of artificial intelligence used in systems for protecting computer networks in transport from cyber attacks.

Keywords: artificial intelligence; cyber attacks; neural networks; inaccurate logic; expert logic; machine learning.

Актуальность темы безопасности для современного общества, в том числе для сферы судоходства, не вызывает сомнений. Аварийные ситуации, случаи и происшествия с пассажирскими и торговыми судами случаются все чаще из-за халатности экипажей, износа технического обеспечения и неподготовленности к информационным атакам. За 2018 год компания Trend Micro заблокировала 48 млрд атак. По данным Positive Technologies количество атак в 2020 году выросло на 59% по сравнению с 2019 годом, а за 2022 год было официально зафиксировано на 7% успешных инцидентов больше, чем в 2021. Увеличивается и количество целевых атак, которые несут колоссальный ущерб компаниям.

В структуре современных методов защиты от кибератак значимое место занимают методы искусственного интеллекта.

Термином «искусственный интеллект» (artificial intelligence) — ИИ (AI) называют область информационных технологий, занимающейся автоматизацией разумного (интеллектуального) поведения. Определяют ИИ как способность автоматических (автоматизированных) систем имитировать человеческие интеллектуальные процессы. Выделяют два подхода к проблеме ИИ: конвенционный и вычислительный [1].

В конвенционном подходе на основе статистического анализа и теории статистических решений строится машинное самообучение системы ИИ. Методы конвенционного ИИ реализуются в экспертных системах, Байесовских сетях доверия и др.

В вычислительном подходе обучение производится значительным числом итераций обработки эмпирических данных. Основу вычислительного ИИ составляют нейронные сети [2-7], нечеткие системы [1, 7], эволюционные вычисления [8-11].

Мощный класс нейронных сетей, который используется при обучении без контроля, представляют порождающие состязательные сети (GAN) [12]. Они являются порождающими моделями в том смысле, что они создают новые данные, которые напоминают исходные обучающие данные. Новые данные создаются на основе изучения закономерностей в исходных данных. Такой алгоритм машинного обучения использует две состязательно обучаемые нейронные сети: генератор и дискриминатор.

Генератор создает новые данные путем сопоставления вектора случайного шума с реалистичным выходным сигналом. Затем дискриминатор обучается различать сгенерированные и реальные данные.

Генератор и дискриминатор обучаются вместе в процессе, называемом состязательным обучением. Во время этого процесса генератор пытается создать данные, которые могут обмануть дискриминатор, в то время как дискриминатор пытается точно определить, являются ли данные реальными или поддельными. Затем выходные данные генератора уточняются на основе обратной связи от дискриминатора, и процесс продолжается до тех пор, пока генератор не сможет выдавать данные, неотличимые от реальных.

AI2 (Adversarial Input Interpretation) — это метод защиты нейронных сетей от враждебных атак. Алгоритм AI2 использует сверточную сеть MMSTV (Makoto Mori Slow Scan TV) и внедряет слой возмущения перед входным слоем в процессе обучения. Этот слой применяет FGSM атаку, чтобы «обучить» модель быть устойчивой к подобным атакам. Таким образом, благодаря этому методу MMSTV становится значительно устойчивее к FGSM атаке.

Для обеспечения доказуемой устойчивости AI2 к FGSM атаке используется классическая структура абстрактной интерпретации. Это позволяет получить надежные, вычислимые и точные конечные приближения потенциально бесконечных наборов поведения нейронных сетей. Абстрактная область состоит из логических формул, описывающих определенные формы, такие как зонотопы и ограниченные формы многогранников.

Ключевой идеей AI2 является переформулирование проблемы анализа нейронных сетей в рамках классической абстрактной интерпретации. Для этого определены абстрактные преобразователи, которые фиксируют поведение обычных слоев нейронной сети, и представлен ограниченный домен (powerset), который обеспечивает компромисс между точностью и масштабируемостью.

Экспериментальные результаты показали, что AI2 может эффективно обрабатывать нейронные сети, которые недоступны существующим методам защиты. Помимо этого, AI2 разрабатывается и дополняется абстрактными преобразователями для поддержки большего количества функций нейронных сетей. Также создается библиотека для моделирования распространенных возмущений, таких как вращение, сглаживание и эрозия. Эти расширения позволят лучше применять AI2 в области информационной безопасности. Метод защиты AI2 от враждебных факторов представлен в исследовании [2].

Метод состязательного обучения, представленный в [13] основан на базе данных MNIST (Modified National Institute of Standards and Technology) и CIFAR-10 (Canadian Institute For Advanced Research). Сетевая архитектура состоит из двух сверточных слоев ReLU (сверточные слои нейронной сети с выправленными активациями линейных единиц), один из которых содержит 32 фильтра размером 3 на 3, а за ним 64 фильтра размером также 3 на 3. Затем слой с максимальным объединением 2 на 2 и отсевом со скоростью 0,25 применяется перед полностью подключенным слоем ReLU с 1024 единицами. Последний уровень — это еще один полностью связанный уровень с 11 блоками и функцией активации softmax для классификации в 10 обычных классов плюс состязательный класс. Используется набор инструментов для обеспечения состязательной надежности для создания состязательных примеров для обучения и тестирования. Из-за ограниченных вычислительных ресурсов авторы используют только атаки BIM (Basic Iteractive Method) и C & W (самые сильные атаки) и гауссов шум для генерации дополнительных изображений для обучения. С помощью этого метода удалось повысить точность классификаторов на тестовых изображениях MNIST и CIFAR-10 и точность классификатора при атаках FGSM, C & W, BIM и DeepFool.

Подводя итоги, отметим необходимость постоянного совершенствования систем безопасности и применения инновационных методов для борьбы с семантическими атаками. Только таким образом можно повысить уровень защиты информационных систем и минимизировать потенциальные угрозы для безопасности данных [14, 15]. Дальнейшие исследования в этой области могут привести к разработке более эффективных методов защиты и обеспечения безопасности в сфере информационных технологий. Было обнаружено, что искусственный интеллект является перспективным инструментом в области информационной безопасности, способным обнаруживать киберугрозы, вредоносные действия и предсказывать потенциальные атаки [3, 5, 6].

Системы искусственного интеллекта, основанные на машинном и глубинном обучении, а также нейронных сетях, имитируют работу биологических нейронных сетей в мозге человека [5]. Они обучаются распознавать вредоносные программы и реагировать на них, а также анализировать данные о киберугрозах для прогнозирования их влияния.

Использование искусственного интеллекта в области информационной безопасности открывает новые возможности для защиты от семантических атак. Он позволяет обнаруживать даже незначительные проявления вредоносных программ или атак вымогателей до их проникновения в систему. Кроме того, анализ данных о киберугрозах позволяет предсказывать потенциальные атаки и принимать соответствующие меры предосторожности.

СПИСОК ЛИТЕРАТУРЫ

1. Полтавцева М. А., Лаврова Д. С. Высокопроизводительные системы обнаружения вторжений. СПб. : Политех-пресс, 2020. 186 с.
2. AI2: Safety and Robustness Certification of Neural Networks with Abstract Interpretation / Timon G. [et al]. // 2018 IEEE Symposium on Security and Privacy (SP). 2018. [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/8418593 (дата обращения: 10.07.2023).
3. Hybrid neural networks in cyber physical system interface control systems / Sokolov S. [et al]. |// Bulletin of Electrical Engineering and Informatics. 2020. Vol. 9. № 3. Pp. 1268-1275.
4. Оптимальная идентификация объектов в задачах распознавания необитаемыми подводными аппаратами / Ныркov А. П. [и др.]. // Проблемы информационной безопасности. Компьютерные системы. 2020. №2 (42). С. 58–64.
5. Tsymay Y. V., Nyrkov A. P., Kardakova M. V. Neurointerface Modeling For Controlling Dynamic Systems // Intellectual Technologies on Transport. 2022. №4. Pp. 85-93.
6. Convolution Neural Network for Identification of Underwater Objects / Sobolev A. S. [et al]. // Proceedings of the 2022 Conference of Russian

Young Researchers in Electrical and Electronic Engineering, EIConRus 2022 9755621. 2022. Pp. 455-458.
7. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы. М. : Горячая линия Телеком, 2006. 452 с.
8. Андреев А. А. Применение генетических алгоритмов при оптимизации нелинейных функций // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2009. Т. 14. № 5-2.
9. Генетические алгоритмы в математическом моделировании перегрузочных процессов / Нырков А. П. [и др.] // Высокие технологии, фундаментальные исследования, образование. Т.2 : Сб. тр. Восьмой международной научно–практической конференции «Исследование, разработка и применение высоких технологий в промышленности». СПб. : Изд–во Политехн. ун–та, 2009. С. 57 — 60.
10. Нырков А. П. Алгоритм размещения партии контейнеров на складской площадке на основе случайного поиска // Сборник научных трудов РАТ Информационные системы на транспорте. СПб. : Судостроение, 2002. С. 231 — 233.
11. Истомин Е. П., Кныш Т. П., Истомин Е. П., Шкадова А. Р. Методы теории вероятностей и математической статистики в моделировании транспортных процессов. СПб. : СПГУВК, 1999. 168 с.
12. Andrei-Grigore M., Daniel Z., Virgil D.. Development of a Machine-Learning Intrusion Detection System and Testing Its Performance Using a Generative Adversarial Network, 2023 [Электронный ресурс]. URL: https://www.researchgate.net/publication/367403291_Development_of_a_Machine-Learning_Intrusion_Detection_System_and_Testing_of_Its_Performance_Using_a_Generative_Adversarial_Network (дата обращения: 10.07.2023).
13. Jing L., Laurent L. N., Kaiqi X. Secure machine learning against adversarial samples at test time [Электронный ресурс]. URL: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-021-00125-2 (дата обращения: 10.07.2023).
14. Нырков А. П., Рудакова С. А. Методика аудита объектов информатизации по требованиям информационной безопасности // Журнал университета водных коммуникаций. 2012. № 3. С. 146-149.
15. Sokolov S. S., Glebov N. B., Antonova E. N., Nyrkov A. P. The Safety Assessment of Critical Infrastructure Control System // Proceedings of the 2018 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», IT and QM and IS, 5 November. 2018. Pp. 154-157.

УДК 004.855.5

МЕТОДЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫХ СЕТЯХ ТРАНСПОРТНОЙ ОТРАСЛИ

Нырков Анатолий Павлович, Юмашева Елена Сергеевна, Нырков Андрей Анатольевич
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: kaf.koib@gmail.com, elena_umasheva@mail.ru, aanyrkow@mail.ru

Аннотация. В работе исследуется возможность использования методов обнаружения вторжений в компьютерных сетях на транспорте.

Ключевые слова: методы обнаружения вторжений; автоматизированные системы; транспортные процессы; классификация методов.

INTRUSION DETECTION METHODS IN COMPUTER NETWORKS OF TRANSPORT INDUSTRY

Nyrkov Anatoliy, Yumasheva Elena, Nyrkov Andrey
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: kaf.koib@gmail.com, elena_umasheva@mail.ru, aanyrkow@mail.ru

Abstract. The paper explores the possibility of using intrusion detection methods in computer networks in transport.

Keywords: intrusion detection methods; automated systems; transport processes; classification methods.

Развитие цифровых технологий, внедрение систем автоматизированного управления технологическими процессами в промышленности, на транспорте и других производствах привели к росту числа угроз безопасности этих процессов, к росту кибератак на автоматизированные системы. Использование компьютерных сетей и интеллектуальных устройств позволили злоумышленникам организовать множество удаленных атак на автоматизированные системы [1]. В последние годы разработано значительное количество систем обнаружения вторжений (СОВ), но предприятия промышленности и транспортной отрасли по-прежнему сталкиваются с успешно проведенными атаками, которые традиционные системы СОВ не могут выявить [2]. Всё это требует создания новых подходов к обеспечению безопасности технологических процессов [3].

Исследование направлено на проведение анализа современных методов обнаружения вторжений.

Всего за 2022 год по данным Positive Technologies было официально зафиксировано на 7 % (223) успешных инцидентов больше, чем в 2021. Среди общего количества атак 97% являлись целевыми. Например, одной из крупных атак в прошлом (2011 год) стала кибератака на иранский ядерный объект. Вредоносное программное обеспечение (далее — ПО) распространилось на все программируемые логические контроллеры (ПЛК), что привело к уничтожению существенного количества центрифуг [4-6].

Атаки на АСУ ТП могут быть как целенаправленные, так и нецеленаправленными. Первый тип атак готовится планомерно, т.е. проводится разведка с помощью инструментов Open Source Intelligence (OSINT), планирование действий (некоторые векторы внедрения в инфраструктуру могут соответствовать матрице MITRE ATT&CK) и подготовка при необходимости к физическому проникновению на объект. Например, одним из рабочих векторов атаки на такие объекты является «подавление функции управления». Так как целевые атаки не проводятся в один этап, то по определенным признакам система может отследить готовящуюся атаку и уведомить специалистов ИБ.

Нецелевые атаки обычно выполняются спонтанно и не имеют цели взломать тот или иной объект. Например, сканирование ботами сети привело к взлому учетной записи пользователя на веб ресурсе или уволенный сотрудник обнаружил, что специалисты IT не забрали у него доступ к корпоративной сети.

Автоматизированные системы обычно разрабатываются так чтобы их информационная безопасность зависела от своей среды. Уязвимые места в работе протоколов закрываются выделенной сетью, контролируемой оператором. Однако не всегда такая реализация возможна. Снижение уровня безопасности в сетях АСУ ТП происходит преимущественно из-за трёх ситуаций:

1. Конвергенция сетей. Сети перестают быть изолированными, взаимодействуют с компонентами автоматизации и, следовательно, область атак увеличивается. Например, если в АСУ ТП появляется облачная платформа, с возможностью управления различными компонентами через смартфон.

2. Устаревшие best practices. Устройства и приложения в среде АСУ ТП предназначены для длительного срока эксплуатации при обычном (рядовом) использовании, а не для устойчивости к сетевым атакам. Несмотря на передовые исследования, выпуск обновлений ПО, во многих средах по-прежнему остаются старые бэкдоры или происходит удаленное администрирование с помощью небезопасных протоколов (FTP, VNC, TeamViewer и др.).

3. Безопасность не является приоритетом в бизнес-процессах, особенно на транспорте. В приоритет ставится работоспособность того или иного приложения из-за чего часто процессы запущены с повышенными привилегиями «все разрешено». Например, инженерные станции, на которых используется ПО для перепрограммирования ПЛК, плохо работают в многопользовательском режиме и должны быть доступны контрагентам в случае проведения плановых работ. Здесь обычные брандмауэры не будут эффективны, и для обнаружения вторжения потребуется понимание трафика на уровне протоколов.

На сегодняшний день существующие методы обнаружения вторжений подразделяют на поведенческие, сигнатурные и основанные на методах искусственного интеллекта [2].

Поведенческие методы анализируют сетевой трафик, применяя различные вычислительные алгоритмы обработки информации: основанные на математической статистике, на вейвлет–анализе и др.

Сигнатурные методы основаны на поиске сигнатур сетевых атак, имеющихся и пополняемых в соответствующих базах данных.

К методам искусственного интеллекта относятся методы машинного обучения и вычислительных интеллектуальных алгоритмов: нейросети [7, 8], метод случайного леса (Random forest) [9]; Бэггинг (bootstrap aggregation) [10] и др. Например, в работе [7] применяется свёрточная нейросеть идентификации подводных объектов.

Эффективность современных подходов не может быть точно оценена из-за ограничений в реальных атаках и датасетах. Также не существует стандартного набора показателей эффективности, благодаря которым было бы возможно измерить эти подходы. Таким образом, становится очевидной необходимость в решении этих проблем не только в рамках разработки более эффективного детектора атак, но и для повышения надежности систем обнаружения вторжений.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы для промышленных организаций: итоги 2022 года // Positive technologies, 2023. [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/industrial-cybersecurity-threatscape-2022/ (дата обращения: 04.07.2023).
2. Полтавцева М. А., Лаврова Д. С. Высокопроизводительные системы обнаружения вторжений. СПб.: Политех-пресс, 2020. 186 с.
3. Ныркov А. П., Соколов С. С., Шнуренко А. А. Автоматизированное управление транспортными системами : монография. СПб.: ГУМРФ им. адмирала С. О. Макарова, 2013. 325 с.
4. Langner R. Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 2011. Vol. 9. Issue 3. Pp. 49–51.
5. LeCun Y., Bengio Y., Hinton G. Deep learning. Nature, 2015. 521(7553). Pp. 436–444.
6. Зубанова А. А., Шипунов И. С., Ныркov А. П. О возможностях применения программируемых логических контроллеров для целей мониторинга состояния судового оборудования // XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020 г. Ч. 1. : материалы конференции. СПб.: СПОИСУ, 2020. С. 345–348.
7. Sobolev A. S. [and others]. Convolution Neural Network for Identification of Underwater Objects / A. S. Sobolev, S. G. Chernyi, A. P. Nyrkov, D. O. Krivoguz, E. G. Zinchenko // Proceedings of the 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus, 2022. Pp. 455-458.
8. Рекуррентные нейронные сети (KTT) с Keras [Электронный ресурс] // Xabr, 2020. [Электронный ресурс]. URL: https://habr.com/ru/articles/487808 (дата обращения: 10.07.2023).
9. Random forest // Анализ малых данных, 2016. [Электронный ресурс]. URL: https://alexanderdyakonov.wordpress.com/2016/11/14/случайный-лес-random-forest (дата обращения: 11.07.2023).
10. Бэггинг // Machinelearning [Электронный ресурс]. URL: http://www.machinelearning.ru/wiki/index.php?title=Бэггинг (дата обращения: 14.07.2023).

УДК 004.01

ПРОГРАММНЫЙ КОМПЛЕКС ГЕНЕРАЦИИ БЕЗОПАСНЫХ ПАРОЛЕЙ

Скобелев Алексей Вячеславович, Голоскоков Константин Петрович
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: skobelevav@gumrf.ru, goloskokovkp@gumrf.ru

Аннотация. В работе проведен критический анализ генераторов паролей freeware. В качестве базового ПО генератора паролей рассмотрен комплекс Windows LAPS. В итоге предложен более удобный, безопасный и гибкий в настройке генератор паролей.

Ключевые слова: генератор паролей; анализ генераторов паролей; автоматизация; Windows LAPS.

SOFTWARE COMPLEX FOR GENERATING SECURE PASSWORDS

Skobelev Alexey, Goloskokov Konstantin
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: skobelevav@gumrf.ru, goloskokovkp@gumrf.ru

Abstract. The paper provides a critical analysis of freeware password generators. The Windows LAPS complex is considered as the basic password generator software. As a result, a more convenient, secure and flexible password generator is proposed.

Keywords: password generator; password generator analysis; automation; Windows LAPS.

В соответствии с современными стандартами на систему менеджмента информационной безопасности в организации должны быть идентифицированы многие факторы, которые требуют управления, поскольку они вызывают риски (положительные и отрицательные). Общим требованием является идентификация факторов риска, оказывающих наибольшее влияние на деятельность организации. Одной из ключевых задач в обеспечении информационной безопасности является управление доступом к паролю локального администратора операционной системы Windows, т.к. это дает полный доступ к компьютерной системе, и может представлять серьезную угрозу для безопасности любой организации [1].

В процессе исследования и анализа генераторов паролей была изучена проблема управления доступом к паролю локального администратора в организациях. Анализ существующих решений, в том числе Windows LAPS [2], показал необходимость построения своего генератора паролей [3].

Были определены функциональные требования к проектируемому программному комплексу, включая механизмы безопасности, автоматизацию процесса выдачи паролей и механизмы аутентификации [4, 5].

В ходе разработки программного комплекса генератора был использован язык программирования Python и библиотека Telegram API для создания Telegram-бота. Тестирование и отладка программного комплекса показали его надежность и криптостойкость генерируемых паролей.

В разработанном генераторе паролей кроме автоматизация процесса выдачи паролей локального администратора операционной системы Windows с использованием Telegram для обмена информацией между администратором и конечным пользователем, обеспечено безопасное хранение паролей локального администратора, что предотвращает утечку или несанкционированный доступ, разработан механизм аутентификации и авторизации пользователей, включающий механизм централизованного контроля доступа, позволяющий определить список авторизованных пользователей, имеющих право получать пароли локального администратора.

Разработанный программный комплекс генерации паролей представляет собой полезное и безопасное решение для обслуживания парка компьютерной техники и управления доступом к паролю локального администратора ОС Windows. Он позволяет упростить процесс выдачи паролей и обеспечивает высокий уровень безопасности. В сравнении с альтернативным решением Windows LAPS, он обладает более гибкой настройкой и доступной стоимостью, что делает его привлекательным выбором для многих организаций. При этом, необходимо учитывать возможные недостатки, связанные с использованием мессенджера Telegram для передачи паролей, и принимать соответствующие меры для обеспечения безопасности данного процесса.

СПИСОК ЛИТЕРАТУРЫ

1. О безопасности критической информационной инфраструктуры Российской Федерации: Фед. закон № 187-ФЗ от 26.07.2017. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 21.07.2023).
2. Что такое Windows LAPS? [Электронный ресурс]. URL: https://learn.microsoft.com/ru-ru/windows-server/identity/laps/laps-overview (дата обращения: 12.05.2023).
3. Нырков А. П., Нырков А. А. Генераторы случайных чисел. СПб.: ГУМРФ им. адм. С. О. Макарова, 2015. 56 с.
4. Ерисова А. Д., Нырков А. П. О применении цифровых сертификатов как средства аутентификации в транспортно-логистических компаниях // XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)» Санкт-Петербург, 28-30 октября 2020 г. : материалы конференции. Ч. 1. СПб. : СПОИСУ, 2020. С. 343–345.
5. Ерисова А. Д., Нырков А. П., Каторин Ю. Ф. О безопасности применения цифровых сертификатов как средства аутентификации в информационных системах на транспорте // Современные тенденции и перспективы развития водного транспорта России, 1 октября 2020 г. : материалы межвузовской научно-практической конференции. Ч. 3. СПб. : Изд-во ГУМРФ им. адм. С. О. Макарова, 2020. С. 70–71.

УДК 004.05 : 004.5

ДИАЛОГОВЫЕ МОДУЛИ «АИС ИТ КЛИНИКА»

Шипунов Илья Сергеевич, Нырков Анатолий Павлович,
Ротнов Дмитрий Александрович, Шипунова Диана Алексеевна
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: shipunovis@gumrf.ru, kaf.koib@gmail.com, erikfrish@gmail.com, shipunovada@gumrf.ru

Аннотация. Рассматриваются аспекты разработки модулей «АИС ИТ клиника» ГУМРФ имени адмирала С. О. Макарова, обеспечивающих диалог с пользователями системы.

Ключевые слова: морской ВУЗ; ИТ; ИТ клиника; АИС; коммуникационные модули.

DIALOGUE MODULES «AIS IT CLINIC»

Shipunov Ilya, Nyrkov Anatoliy, Rotnov Dmitry, Shipunova Diana
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: shipunovis@gumrf.ru, kaf.koib@gmail.com, erikfrish@gmail.com, shipunovada@gumrf.ru

Abstract. The aspects of modules development of the «AIS IT Clinic» of the Admiral Makarov SUMIS, providing a dialogue with users of the system.

Keywords: Maritime University; IT; IT clinic; AIS; communication modules.

АИС «ИТ Клиника» призвана обслуживать целый ряд различных пользователей, для каждого из которых необходимо предусмотреть свой уникальный функционал. Эти пользователи подразделены на следующие группы: «Администратор», «Управляющий», «Заказчик», «Исполнитель», «Наставник». Для каждого из этих типов пользователей внутри системы создаются специализированные разделы, содержащие набор определенных инструментов. Подобная структура позволяет сделать систему максимально функциональной и удобной для конечного пользователя [1-3].

Каждый инструмент в итоговой АИС представляет собой отдельную вкладку в web-приложении, отвечающую за выполнение определенных функций. Так, например, раздел «Администратор» включает в себя инструменты, позволяющие настраивать и модифицировать работу системы, раздел «Управляющий» содержит инструменты для контроля и управления процессом выполнения задач, раздел «Заказчик» позволяет формировать и подавать новые задачи и т.д. Такой подход делает систему гибкой и масштабируемой, позволяя легко вносить изменения и расширять функционал при необходимости [4-6].

В течение процесса разработки были реализованы модули «Бот», «Почта», «Геолокация», «Генерация отчетов». Эти модули были названы именно так, поскольку их создание проводилось автономно, без участия других разработчиков, и они не были привязаны к определенным разделам системы, обладая возможностью использования в различных его частях, а некоторые вообще работают независимо от основной системы.

Модули «Бот» и «Почта» созданы для оперативного информирования пользователей об изменении статуса задач или других важных событиях в системе. Это может быть, например, уведомление об изменении статуса задачи.

Модуль «Геолокация» реализован для определения географического положения исполнителей. Это необходимо для оценки их возможности взять на себя выполнение задачи, требующей присутствия на территории университета.

Модуль «Генерация отчетов» способен формировать различные виды отчетности и документов на основе предварительно загруженных в систему шаблонов. Вывод информации осуществляется в формате документа *.docx, что упрощает дальнейшую работу с ними. Один из ключевых типов отчетов — это отчет об активности исполнителей, который позволяет руководству вовремя определять факты простоя некоторых сотрудников и принимать соответствующие меры. Также на основе данного отчета формируются списки наиболее активных исполнителей для награждения и стимулирования их работы.

Для реализации проекта АИС «ИТ Клиника» необходимо было тщательно выбрать определенные технологии, языки программирования и расширения [7, 8]. Это обусловлено тем, что разработка велась в модульном стиле, следовательно, каждый модуль имел свои специфические требования, которые определяли выбор соответствующих инструментов.

Модуль «Бот» был создан с использованием языка программирования Python 3.11 и асинхронной библиотеки aiogram 3.0. Библиотека aiogram основывается на aiohttp и обеспечивает возможность написания эффективных и производительных ботов для Telegram.

Модуль «Почта» был реализован на языке PHP. Для отправки сообщений от собственного доменного имени использовался сервер iRedMail. Это решение позволило обеспечить уверенную и надежную работу функционала почты.

Модуль «Геолокация» был разработан на языке JavaScript. Этот скрипт обеспечивает доступ к текущему местоположению пользователя с помощью встроенного функционала браузеров. Обработка запроса с позицией пользователя на стороне сервера осуществлялась с использованием PHP.

Модуль «Генерация отчетов» был создан с использованием языка PHP, менеджера пакетов Composer и библиотеки phpword версии 1.0.

Важным аспектом разработки было обеспечение эффективного сотрудничества всех участников команды разработчиков. Для этого был создан специальный сервер на основе GitLab Community Edition. Он служил централизованной платформой для управления кодом, предоставляя доступ к нему только участникам команды разработчиков.

СПИСОК ЛИТЕРАТУРЫ

1. Ныркov А. П., Соколов С. С., Башмаков А. В. Методика проектирования безопасных информационных систем на транспорте // Проблемы информационной безопасности. Компьютерные системы. 2010. № 3. С. 58-61.
2. Методы обеспечения информационной защищенности данных электронной информационно-образовательной среды университета / Соколов С. С. [и др.] // Региональная информатика и информационная безопасность. СПб.: СПОИСУ, 2017. Вып. 4. С. 309–312.

3. Search methods for abnormal activities of web applications / Mikheeva O. I. [et all] // Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 2020. Vol. 20, no. 2, 2020. Pp. 233–242. https://doi.org/10.17586/2226-1494-2020-20-2-233-242.
4. Соколов С. С., Ныркова А.П. Концепция и модель построения безопасного единого пространства информационного обмена между автоматизированными системами управления объектами транспортной инфраструктуры // Перспективные направления развития отечественных информационных технологий. Материалы III межрегиональной научно-практической конференции. 2017. С. 41-44.
5. Data structures access model for remote shared memory / Nyrkov A. P. [et all] // E3S Web of Conferences 244. 2021.
6. Nyrkov A. A., Romanova Y. N., Ianiushkin K. A., Li I. V. Data Processing Model in Hierarchical Multi-agent System Based on Decentralized Attribute-Based Encryption // Advances in Intelligent Systems and Computing, Vol. 982. 2020. Pp. 429-438.
7. Ныркова А. П., Ныркова А. А. Сравнительная оценка математического обеспечения систем управления базами данных // Задачи контроля и управления. СПб. : СПГУВК, 1997. С. 142-145.
8. Ныркова А. А., Ныркова А. П. Автоматизация информационного обеспечения деятельности исследовательской проблемной лаборатории // Управление транспортными системами. СПб. : СПГУВК, 1997. С. 98-99.

УДК 004.05 : 004.5

О ЗАЩИЩЕННОСТИ КОММУНИКАЦИОННЫХ МОДУЛЕЙ «АИС ИТ КЛИНИКА»

Шипунов Илья Сергеевич, Ныркова Анатолий Павлович, Шипунова Диана Алексеевна
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: shipunovis@gumrf.ru, kaf.koib@gmail.com, shipunovada@gumrf.ru

Аннотация. Предложены подходы к обеспечению защищенности работы приложения «АИС ИТ клиника» при использовании модулей бот, почта, геолокация, отчеты.

Ключевые слова: защита веб-приложения; SSL/TLS; DDoS; SQL-инъекции; Content Security Policy; xss; GitLab.

ON THE SECURITY OF THE COMMUNICATION MODULES «AIS IT CLINIC»

Shipunov Ilya, Nyrkov Anatoliy, Shipunova Diana
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 7198035, Russia
e-mails: shipunovis@gumrf.ru, kaf.koib@gmail.com, shipunovada@gumrf.ru

Abstract. Approaches are proposed to ensure the security of the application «AIS IT Clinic», when using modules bot, mail, geolocation and reports.

Keywords: web application protection; SSL/TLS; DDoS; SQL injection; Content Security Policy; xss; GitLab.

Серверное программное обеспечение является критическим звеном для обеспечения безопасности веб-приложения. Использование последних версий операционных систем, веб-серверов и систем баз данных, а также своевременное обновление этого ПО для устранения известных уязвимостей, помогает обеспечить его безопасность [1, 2]. Кроме того, применение технологий шифрования передачи данных, таких как SSL/TLS, и средств защиты от DDoS-атак помогает уберечь сервер от прямых атак и обеспечить его надежную работу.

Обеспечение безопасности на уровне приложения включает в себя создание безопасного кода, включая валидацию ввода, использование параметризованных запросов для предотвращения SQL-инъекций, и применение безопасных API и библиотек. Важной составляющей является также система аутентификации и авторизации для контроля доступа к функциям веб-приложения, которая может использовать сессии, токены, двухфакторную аутентификацию и контроль доступа на основе ролей [3-5].

Защита баз данных направлена на обеспечение безопасности хранящихся в ней данных [6, 7]. Использование шифрования, резервного копирования и контроля доступа помогает обеспечить целостность и конфиденциальность данных [8-11]. Предотвращение SQL-инъекций с помощью параметризованных запросов и валидации ввода, а также мониторинг и аудит для выявления подозрительной активности также являются важными составляющими защиты баз данных [12, 13].

Безопасность на уровне пользовательского интерфейса обеспечивается применением различных мер на стороне пользователя. Использование HTTPS для безопасной передачи данных, токенов CSRF для защиты от межсайтовой подделки запросов и Content Security Policy (CSP) для защиты от межсайтового скриптинга важны для обеспечения безопасности взаимодействия пользователя с приложением.

Кроме того, реализация функционала, позволяющего пользователям контролировать и управлять своими личными данными в соответствии с GDPR, является ключевым элементом защиты приватности.

Файрволлы веб-приложений (WAF) являются еще одним важным компонентом защиты веб-приложений. Они функционируют на уровне приложений, мониторя и фильтруя весь входящий трафик на предмет атак, таких как SQL-инъекции, межсайтовый скриптинг (XSS) и межсайтовая подделка запроса (CSRF), помогая таким образом обеспечивать безопасность приложения от различных веб-угроз.

Безопасный дизайн начинается с тщательного планирования и учета потенциальных угроз веб-приложению еще на стадии проектирования. Основные принципы безопасного дизайна включают минимизацию поверхности атаки, применение принципа наименьших привилегий, использование защиты на многоуровневой основе и предусмотрение безопасности «по умолчанию».

Минимизация поверхности атаки означает, что в веб-приложении следует иметь только те функции и компоненты, которые действительно необходимы, чтобы ограничить возможные точки входа для атак. Принцип

наименьших привилегий означает, что каждый компонент веб-приложения должен иметь только те привилегии, которые ему действительно необходимы для выполнения своих функций. Многоуровневая защита означает использование нескольких слоев защиты для обеспечения безопасности в случае прорыва одного из слоев. Безопасность «по умолчанию» означает, что безопасные настройки и практики должны быть встроены в веб-приложение с самого начала.

Разработка безопасных веб-приложений требует использования методологий, которые включают в себя безопасность на каждом этапе процесса разработки. Например, методология безопасной разработки по жизненному циклу (SDLC) подразумевает включение процессов обеспечения безопасности на этапах планирования, проектирования, разработки, тестирования и обслуживания веб-приложения.

При разработке системы АИС «ИТ-Клиника» основной код был размещен на собственном сервере GitLab. Это позволило обеспечить контроль над исходным кодом и предотвратить его нежелательное распространение. Важным аспектом безопасной разработки является также проведение регулярных аудитов кода и пентестов для обнаружения и устранения уязвимостей.

Существуют различные инструменты и практики, которые можно использовать для обеспечения безопасности веб-приложения. Это может включать в себя использование систем управления версиями, таких как Git, для контроля изменений в исходном коде, использование инструментов статического анализа кода для обнаружения уязвимостей, использование систем автоматизации тестирования для обеспечения качества кода и использование систем управления конфигурациями для обеспечения стабильности и надежности веб-приложения.

Среди практик безопасности стоит отметить регулярное обновление и патчинг программного обеспечения, следование принципам безопасного кодирования, проведение регулярных аудитов безопасности и проведение обучения по безопасности для разработчиков.

СПИСОК ЛИТЕРАТУРЫ

1. Search methods for abnormal activities of web applications / Mikheeva O. I. [et all] // Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2020. Vol. 20. № 2. Pp. 233–242.
2. Ныркov А. П., Соколов С. С., Башмаков А. В. Методика проектирования безопасных информационных систем на транспорте // Проблемы информационной безопасности. Компьютерные системы. 2010. № 3. С. 58-61.
3. Ерисова А. Д., Ныркov А. П. Возможности цифровых сертификатов при аутентификации // «Информационные управляющие системы и технологии» (ИУСТ–Одесса–2020) : Материалы IX международной научно-практической конференции. Одесса, 2020. С. 87–91.
4. Ерисова А. Д., Ныркov А. П., Каторин Ю. Ф. О безопасности применения цифровых сертификатов как средства аутентификации в информационных системах на транспорте // Современные тенденции и перспективы развития водного транспорта. Материалы XII межвузовской научно-практической конференции аспирантов, студентов и курсантов. 01 октября 2020 года: Часть 3. СПб. : Изд-во ГУМРФ им. адм. С. О. Макарова, 2020. С. 70–71.
5. Ерисова А.Д., Ныркov А.П. О применении цифровых сертификатов как средства аутентификации в транспортно-логистических компаниях // информатика (РИ-2020). Часть 1. Санкт-Петербург, 28-30 октября 2020. СПб. : СПОИСУ, 2020. С. 343–345.
6. Databases Problems for Maritime Transport Industry on Platform Highload / Nyrkov A. P. [et all] // Proceedings of the 2018 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», IT and QM and IS 5 November 2018. Pp. 132-135.
7. Ныркov А. П., Ныркov А. А. Сравнительная оценка математического обеспечения систем управления базами данных // Задачи контроля и управления. СПб. : СПГУВК, 1997. С. 142-145.
8. Ныркov А. П., Романова Ю. Н., Янюшкин К. А. К вопросу о применении отечественных алгоритмов шифрования // Региональная информатика и информационная безопасность. Вып. 2 СПб. : СПОИСУ, 2016. С. 117–120.
9. Ныркov А. П., Черняков А. В. Алгоритмы резервного копирования для обеспечения защиты данных // Информационная безопасность регионов России (ИБРР–2015). СПб. : СПОИСУ, 2015. С. 127 — 128.
10. Ныркov А. П., Черняков А. В. Дедупликация данных в системах резервного копирования // «Информационные управляющие системы и технологии» (ИУСТ–Одесса–2015) : Материалы международной научно-практической конференции, 22-24 сентября 2015 г. Одесса, 2015. С. 130–133.
11. Ныркov А. П., Вайгандт Н. Ю. Контроль целостности данных при мониторинге транспортных средств // Журнал университета водных коммуникаций. 2013. № 1. С. 54-61.
12. Методы поиска аномальных активностей веб-приложений / Михеева О. И. [и др.] // Научно-технический вестник информационных технологий, механики и оптики. Т. 20, № 2. 2020. С. 233–242.
13. Ныркov А. П., Рудакова С. А. Методика аудита объектов информатизации по требованиям информационной безопасности // Журнал университета водных коммуникаций. 2012. № 3. С. 146-149.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

УДК 681.3.06

IS-АСПЕКТ ИНФОРМАЦИОННО-ПОИСКОВЫХ СИСТЕМ

Азикова Анна Евгеньевна, Озерова Ксения Викторовна, Данильчик Андрей Александрович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mails: anutaazikova@mail.ru, kozierova@mail.ru, danilchikandrey16@gmail.com

Аннотация. Рассмотрены базовые понятия и технологии информационно-поисковых систем, обобщены их задачи и функции, а также информационные уязвимости и угрозы. Обоснована необходимость сочетания их интенсивного развития с разработкой соответствующих организационно-правовых и технологических решений по обеспечению требований ФЗ-152 при использование информационно-поисковых систем различного назначения, включая информационно-коммуникационные и социальные сети и сервисы.

Ключевые слова: пользователь; модератор; регламенты IS; уязвимости; угрозы безопасности.

IS-ASPECT OF INFORMATION SEARCH ENGINES

Azikova Anna, Ozerova Ksenia, Danilchik Andrey
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 190121, Russia
e-mails: anutaazikova@mail.ru, kozierova@mail.ru, danilchikandrey16@gmail.com

Abstract. The basic concepts and technologies of information retrieval systems are considered, their tasks and functions are summarized, as well as information vulnerabilities and threats. The necessity of combining their intensive development with the development of appropriate organizational, legal and technological solutions to meet the requirements of FZ-152 when using information search systems for various purposes, including information and communication and social networks and services, is substantiated.

Keywords: user; moderator; IS regulations; vulnerabilities; security threats.

В настоящее время информационные технологии используются практически во всех сферах жизнедеятельности человека. Уровень использования информационных технологий считается определяющим фактором развития общества, его информационной зрелости.

Вместе с тем, большой объем циркулирующей информации в сетях и используемый при обработке, обуславливает острую необходимость совершенствования соответствующих информационно-поисковых технологий и систем (ИПС), расширения спектра и систем используемых критериев (фильтров) при отборе информации. По определению ИПС — это система, обеспечивающая поиск и отбор необходимых данных в специальной базе с описаниями источников информации (индексов) на основе информационно-поискового языка и соответствующих правил поиска [1].

Сегодня к ИПС относят большое число автоматизированных систем управления обработкой данных. Их основное назначение — сбор и поиск информации и ее представление в удобной пользователю форме. В соответствии с этим назначением основными методами ИПС являются методы поиска и первичной обработки информации [2]. Основной задачей ИПС является поиск и считывание запрошенной пользователями-заказчиками информации, которая, как правило, впоследствии применяется ими для принятия решений [3].

И именно этот процесс в аспекте Informychtn Secyuriti (в контексте информационной безопасности, ИБ) может рассматривать как один из важнейших источников информации для аналитической обработки данных с целью анализа и синтеза (моделирования) образа (цифровой модели) Пользователя, формирования его профессионального и личностного «профиля» (цифрового портрета, цифрового двойника, цифровой тени).

В качестве собирательного образа Пользователя могут выступать физические и/или юридические лица, либо их группы и соответствующие их комбинации. Соответственно, в IS-аспекте и IS-контексте ИПС следует рассматривать в качестве критически важной информационной уязвимости и критической IS-угрозы для Пользователя в случае нарушения организацией, предоставляющей сервис ИПС, будем называть его Модератором, принятого регламента обработки информации и предоставления сервиса.

В этой связи, каждого из подобных модераторов-нарушителей можно рассматривать как субъекта ведения информационной разведки (шпионажа) с соответствующей целью (коммерческой, технологической, социальной,

корпоративной, групповой и т.п.). При этом организация соответствующих дорогостоящих ЦОДов (центров обработки данных, как правило, с заграничной геолокацией) с предоставлением многочисленных бесплатных сервисов (типа Mail, Google, Yandex, WhatsApp, VK, КонсультантПлюс) может рассматриваться, как один из элементов соответствующего системного решения.

Технологически в работе ИПС поисковый процесс представлен четырьмя стадиями [4]: формулировка (происходит до начала поиска); действие (начинающийся поиск); обзор результатов (результат, который Пользователь видит после поиска); усовершенствование (после обзора результатов и перед возвращением к поиску с иной формулировкой той же потребности).

В целом ИПС выполняет следующие функции [1]: хранение больших объемов информации; быстрый поиск требуемой информации; добавление, удаление и изменение хранимой информации; вывод информации в удобном для Пользователя виде.

Общим для ИПС является то, что они размещаются на специально выделенных мощных серверах ЦОД и присоединены к высокоэффективным каналам связи. Такие системы отличаются огромными сервисными возможностями. Так, например, количество одновременно обслуживаемых Пользователей (посетителей) может достигать многих тысяч, а наиболее известные ИПС обслуживают в сутки миллионы Пользователей.

Информационно-поисковые системы с полнотекстовым поиском основываются на автоматическом сборе информации. Он производится специализированными программами, которые периодически просматривают содержимое всех ресурсов Интернета. Для этого они самостоятельно передвигаются или, как говорят, «ползают» по различным информационным ресурсам. Поэтому подобные программы называют роботами. Существуют и иные названия: так как «WWW является аббревиатурой названия «Всемирная паутина», то подобную программу следует назвать спайдером (по-англ. — паук).

В настоящее время применяются и другие названия: автоматические индексы или директории. Все эти программы просматривают и скачивают информацию с разных URL-адресов, посещая соответственно каждый ресурс через установленное время. Естественно, что любая поисковая система не может проиндексировать весь Интернет. Следствием этого является то, что базы данных (БД), в которые помещены адреса проиндексированных ресурсов, у различных ИПС разные. Несмотря на это, многие из поисковых систем пытаются, по возможности, охватывать в своей работе все информационное пространство глобальной сети Интернет. Подобные системы относятся к классу универсальных.

Проведенный анализ позволяет утверждать, что работа поисковой системы основывается на трех составляющих [5]:

– программа «робот» (спайдер), которая проводит анализ информационных ресурсов и осуществляет их индексацию;

– индексы, создаваемые поисковой системой. Они обеспечивают формирование собственных БД;

– программа, которая в соответствии с запросом пользователя готовит ему ответ на основе анализа индексов, т. е. собственных БД.

В действительности Пользователь практически общается только с последней из этих трех составляющих.

Мощные ИПС универсального типа разработаны для работы на всех основных языках мира. Каждая страна стремится разработать свои собственные поисковые системы. В России наибольшей популярностью пользуются следующие поисковые системы [6]:

1. ЯНДЕКС (http://www.yandex.ru) является устойчивым лидером русского сегмента Интернета. Доля данной ИПС в поисковом рынке составляет 54,1 %. Данная IT-компания достаточно быстро развивается, обладает собственными алгоритмами поиска и показателем ранжирования сайтов — ТИЦ.

2. GOOGLE (http://www.goggle.com) является лидером мирового информационного пространства и крупнейшей поисковой системой в мире, но в отечественном сегменте этот гигант так и не смог захватить лидерство и располагается на 2 месте в рейтинге, занимая большую долю рынка — 35,1 %.

3. SEARCH.MAIL.RU. Поисковый сервис от компании Mail.ru находится на 3 месте в рейтинге лучших поисковых систем русского сегмента Интернета, занимая 8,3 % рынка. Компания Mail.ru с момента своего образования реализовывала только почтовый сервис, но в настоящее время она предоставляет, кроме него, еще 40 крупных сервисов, в том числе и поисковый.

4. RAMBLER (http://www.rambler.ru). Рамблер является востребованной поисковой системой, занимая 4 место в рейтинге лучших поисковых систем. Рамблер разработан и запущен российскими учеными в 1997 году, в настоящее время она занимает 0,8 % российского поискового рынка.

5. BING (https://www.bing.com/). Данная поисковая система занимает 5 место в рейтинге лучших поисковых систем русского сегмента Интернета. В настоящее время она занимает 0,6% российского поискового рынка.

Адреса наиболее популярных поисковых систем за рубежом [6]: Google — www.google.com; Altavista — www.altavista.com; Excite — www.excite.com; HotBot — www.hotbot.com; Nothern Light — www.northernlight.com; Go (Infoseek) — www.go.com (infoseek.com); Fast — www.alltheweb.com.

Выполненный анализ IS-аспекта информационно-поисковых технологий и систем позволяет утверждать, что в сочетании с их интенсивным развитием заслуживает особого внимания и разработки соответствующих организационно-правовых и технологических решений по обеспечению требований ФЗ-152 при использовании ИПС различного назначения, включая информационно-коммуникационные и социальные сети и сервисы.

СПИСОК ЛИТЕРАТУРЫ

1. Информационно-поисковые системы [Электронный ресурс]. URL: https://zabai.ru/Load/Kolledj/Metodichki/10.pdf (дата обращения: 22.05.2023).
2. Алексеев А. В. Информационные технологии в жизненном цикле морской техники: курс лекций. СПб. : СПбГМТУ, 2023.
3. Цехановский В. В., Чертовской В. Д. Распределенные информационные системы: учебник для СПО. 2-е, стер. СПб. : Лань, 2021. С. 16. URL: https://e.lanbook.com/book/162391 (дата обращения: 27.05.2023). Режим доступа: для авториз. пользователей.
4. Иванова О. В., Иванов П. В., Смелов М. Н. Алгоритмы и принципы работы поисковых интернет-машин [Электронный ресурс] // T-Comm. 2010. № 10. URL: https://cyberleninka.ru/article/n/algoritmy-i-printsipy-raboty-poiskovyh-internet-mashin (дата обращения: 28.05.2023).
5. Костюк А. В., Бобонец С. А., Флегонтов А. В., Черных А. К. Информационные технологии. Базовый курс: учебник для вузов [Электронный ресурс]. СПб. : Лань, 2021.С. 505. URL: https://e.lanbook.com/book/180821 (дата обращения: 27.05.2023). Режим доступа: для авториз. пользователей.
6. Информационно-поисковые системы и их классификация [Электронный ресурс]. URL: http://www.ta4927570.narod.ru/IPS.html (дата обращения: 22.05.2023).

УДК 629.12, 65.011, 681.518

МЕТОДОЛОГИЯ СОЗДАНИЯ И УЧЕБНО-ЛАБОРАТОРНОГО ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ДВОЙНИКОВ СИСТЕМ АВТОМАТИЗАЦИИ СУДОВ И АУДИТА ИХ ИНФОРМАЦИОННОЙ ЗАЩИЩЕННОСТИ

Алексеев Анатолий Владимирович, Согонов Сергей Александрович, Максимова Марина Александровна, Хруцкий Олег Валентинович, Равин Александр Александрович, Михальчук Андрей Васильевич

Санкт-Петербургский государственный морской технический университет

Лоцманская ул., 3, Санкт-Петербург, 194064, Россия

e-mails: iapbgks@bk.ru, sogonov@mail.ru, maximovama@yandex.ru, obx47@mail.ru, ravinki@mail.ru, 335mav@mail.ru

Аннотация. Роботизация управления системами автоматизации судов в защищенном исполнении (САСЗИ) сегодня является одним из основных направлений повышения их проектного качества и эффективности эксплуатации. В интересах формирования, создания и эффективного использования учебно-лабораторного и исследовательского комплекса (УЛИК) рассмотрена проблема опережающего обучения на основе разработки и исследования возможностей цифровых двойников (ЦД) САСЗИ. С этой целью исследованы перспективные направления развития теории и практики ЦД в судостроении, разработана типовая структура и алгоритм решения комплекса задач автоматизации судов, аудита их информационной защищенности. Разработанное типовое организационно-техническое решение на базе роботизированного проектного комплекса «КАСОР-2023» легло в основу методики выполнения обучаемыми соответствующих лабораторных работ в составе УЛИК, каждая из которых адаптируется к соответствующему классу судов. Обобщен опыт и обоснованы рекомендации по наращиванию возможностей учебно-лабораторного и исследовательского использования и методологии развития ЦД САСЗИ.

Ключевые слова: роботизация управления качеством и эффективностью; технология КАСОР; оптимизация решений; мониторинг управления; типовое решение цифрового двойника.

METHODOLOGY OF CREATION AND EDUCATIONAL AND LABORATORY USE DIGITAL COUNTERPARTS OF SHIP AUTOMATION SYSTEMS AND AUDIT OF THEIR INFORMATION SECURITY

Alekseev Anatoly, Sogonov Sergey, Maximova Marina, Khrutsky Oleg, Ravin Alexander, Mikhalchuk Andrey

Saint Petersburg State Maritime Technical University

3 Lotsmanskaya St, St. Petersburg, 194064, Russia

e-mails: iapbgks@bk.ru, sogonov@mail.ru, maximovama@yandex.ru, obx47@mail.ru, ravinki@mail.ru, 335mav@mail.ru

Abstract. Robotization of control of ship automation systems in protected execution (ASSI) is one of the main directions of improving their design quality and operational efficiency today. In the interests of the formation, creation and effective use of the educational, laboratory and research complex (UIC), the problem of advanced training based on the development and research of the capabilities of digital twins (CD) of SASSI is considered. To this end, promising areas of development of the theory and practice of the CD in shipbuilding have been investigated, a standard structure and algorithm for solving a complex of tasks of ship automation and a comprehensive audit of their information security have been developed. The developed standard organizational and technical solution based on the robotic design complex «KASOR-2023» is the basis for the methodology of performing appropriate laboratory work by trainees as part of evidence, each of which adapts to the appropriate class of vessels. The experience is summarized and recommendations are substantiated on increasing the possibilities of educational, laboratory and research use and methodology of development of CD SASZI.

Keywords: robotization of quality and efficiency management; CASOR technology; optimization of solutions; management monitoring; a typical digital twin solution.

Совершенствование управления системами автоматизации судов в защищенном исполнении (САСЗИ) с переходом к технологиям роботизации и контролируемым обеспечением информационной безопасности используемых данных (ИБ) сегодня является одним из основных направлений повышения их проектного качества и эффективности эксплуатации [1]. Среди ряда нейтрализуемых при этом факторов — негативное влияние субъективных свойств операторов, а также существенный рост возможностей доступа к защищаемым ресурсам в связи с интенсивным развитием и многообразий современных информационных технологий [2].

Эти и ряд других обстоятельств обуславливают ряд проблем подготовки специалистов в области автоматизации судов, включая [1, 2]: проблему модернизации учебно-лабораторной базы в условиях быстро меняющего парка используемых средств и их номенклатуры (сокращения длительности жизненного цикла в условиях интенсивного технологического развития), а также высокой их стоимости; проблему успешного освоения в заданное время, сокращенное с переходом на болонскую систему, широкого спектра и структурно-функциональной сложности вновь появляющихся на рынке средств автоматизации, включая качественно новые технологии и средства обеспечения ИБ; проблему снижения качества документального представления средств и систем автоматизации, даже, при внедрении перспективных технологий создания интерактивных электронных технических руководств; проблему полноты и качества проверки соответствия декларируемых характеристик и параметров в условиях введения новых регламентов технического регулирования в стране, сертификации продуктов и услуг; проблему противоречия между тенденцией резкого возрастания сложности создаваемых САЗИ и тенденцией снижения уровня довузовской подготовки обучаемых.

В определенной мере решить «клубок» возникших проблем позволяет реализация концепции опережающего обучения, ориентированная на ускоренное вовлечение обучаемых в проектную деятельность с соответствующей мотивацией творческой активности и инициативы [3]. В том числе, на основе таких инновационных форм, как, например, создание на Кафедре судовой автоматики и измерений (КСАиИ) СПбГМТУ Центра освоения технологий информационного противоборства (ЦОТИП), а также создание в СПбГМТУ по аналогии с другими ВУЗами такой новой структуры, как Центр трансфера технологий (ЦТТ). В интересах формирования, создания и эффективного использования учебно-лабораторного и исследовательского комплекса (УЛИК), реализуемого на КСАиИ СПбГМТУ в рамках ЦОТИП (с 2020 г.) и ЦТТ (с 2022 г), в докладе рассмотрен вариант реализации проблемы опережающего обучения на основе разработки и исследования возможностей цифровых двойников (ЦД) САСЗИ. С этой целью исследованы перспективные направления развития теории и практики ЦД в судостроении, разработана методология, типовая структура и алгоритм решения комплекса задач автоматизации судов, включая задачу комплексного аудита информационной защищенности САЗИ на основе [2, 3]: технологии квалиметрического анализа, синтеза и оптимизации альтернативных вариантов проектирования и эксплуатации подсистем/системы комплексной защиты информации (СКЗИ) в составе АСЗИ; типизации вариантов построения и модельного представления СКЗИ САЗИ с обоснованием соответствующей системы свойств, критериев и показателей качества; обоснования системы оценки проектного качества и эффективности эксплуатации, а также методов и алгоритмов агрегирования показателей качества, анализа, синтеза и оптимизации, включая показатели конкурентной способности, перспективности развития, инновационных и инвестиционных рисков; технологии информационно-аналитической и интеллектуальной поддержки принятия решений с переходом к технологии роботизации, верификации и валидации решений, целеполагания и риск-менеджмента; технологии цифрового моделирования и мониторинга процессов проектного обоснования и эффективности эксплуатации на основе адаптации и реализации типового решения цифрового двойника. Типовое решение ЦД включает [4] модуль цифрового паспорта (цифрового профиля, цифровой тени), модуль цифрового образа (модели), модуль цифрового двойника, модуль специализированной базы данных и знаний ЦД, модуль поддержки принятия решений и управления (СПРУ) цифровым двойником СКЗИ САЗИ.

Разработанное типовое организационно-техническое решение, реализованное на базе роботизированного проектного комплекса (РПК) «КАСОР-2023» [4], легло в основу методики выполнения обучаемыми соответствующих лабораторных работ УЛИК, каждая из которых адаптируется к своему классу судов. При этом принято целесообразным реализацию представленной методологии начать с типового модуля СКЗИ полномасштабного решения задач ИБ из 12 модулей в составе САСЗИ, что позволит расширить специализацию ЦД САЗИ при использовании СКЗИ в масштабируемом типовом варианте. Обобщение опыта проведения лабораторных работ по технологии ЦД позволило обосновать рекомендации по наращиванию возможностей УЛИК и методологии развития ЦД САСЗИ в направлениях:

– использования комплекса лабораторных работ в составе УЛИК для опережающего освоения в составе ЦОТИП и ЦТТ типового (базового) набора (комплекта) перспективных технологий с последующим инновационным поиском новых конкурентно способных решений при оперативной возможности количественной оценки, анализа, синтеза и оптимизации их конкурентной способности, перспективности развития в сравнении с базовыми (типовыми) организационно-технологическими решениями;

– актуализации базы данных и знаний соответствующих типов ЦД САСЗИ путем включения в нее ЦД новых решений после верификации и оценки их валидности с использованием модуля цифрового паспорта;

– формирования и обоснования системы перспективных направлений технологического развития САСЗИ на основе методов исследовательского проектирования с анализом корневой чувствительности и синтезом приоритетных вариантов их создания.

Таким образом, методология, перечисленные методы и средства создания ЦД САСЗИ на базе РПК «КАСОР-2023» позволяют реализовать в составе УЛИК эффективную систему построения инструментальной среды поддержки учебного процесса, опережающего обучения будущих разработчиков информационных систем автоматизации судов, в том числе основам технологий аудита их информационной защищенности.

СПИСОК ЛИТЕРАТУРЫ

1. Прорывные технологии морских автоматизированных систем в защищенном исполнении / Согонов С. А. [и др.]. // Актуальные проблемы морской энергетики: материалы одиннадцатой международной научно-технической конференции. СПб. : Изд-во СПбГМТУ, 2022. С. 69-77.
2. Алексеев А. В. Информационная живучесть судна: понятие, проблемы, технологии // Региональная информатика и информационная безопасность. Сборник трудов. СПб. , 2019. Вып. 7. С. 345-348.
3. Повышение уровня профессиональной подготовки обучаемых за счет повышения цифровой зрелости учебно-лабораторных комплексов / Согонов С. А. [и др.] // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Санкт- Петербург, 26-28 октября 2022 г. : Материалы конференции. СПб. : СПОИСУ, 2022. С. 464-465.
4. Алексеев А. В., Михальчук А. В. Цифровой двойник системы комплексной защиты информации в инвариантном исполнении (ЦД СКЗИ) // Свидетельство о государственной регистрации программ для ЭВМ (Реестр ФСИС) № 2014613622. 01.04.2023 (06.02.2014).

УДК 629.12, 65.011, 681.518

ЦИФРОВИЗАЦИЯ САМОКОНТРОЛЯ ОСВОЕНИЯ ТЕХНОЛОГИЙ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА ПРИ ОПЕРЕЖАЮЩЕМ ОБУЧЕНИИ

Алексеев Анатолий Владимирович[1], Михальчук Андрей Васильевич[1], Мусатенко Роман Иванович[2]
[1]Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 194064, Россия
[2]ВУНЦ ВМФ «Военно-морская академия им. Н. Г. Кузнецова»
Ушаковская наб., 17/1, Санкт-Петербург, 197045, Россия
e-mails: iapbgks@bk.ru, 335mav@mail.ru, rus-euro-roman@yandex.ru

Аннотация: Среди системных аспектов концепции и методологии опережающего обучения особое место принадлежит подготовке и успешному переходу обучаемого к самообучению и самоконтролю. Среди множества факторов при подготовке по направлению «Информационная безопасность» — высокая динамика и сложность технологического развития, роста профессиональных требований. При безусловной информационно-методической и технологической поддержке выпускника ВУЗа, при формировании модели профессионального и карьерного роста, при профориентировании и целеполагании обоснование и цифровизация ожидаемых показателей и контрольных точек саморазвития являются обязательными при планировании. На примере использования программного комплекса «ЦМПК» показано, что сочетание непрерывного мониторинга результатов самообучения, проектной и публикационной активности цифровизация самоконтроля профессионального и карьерного роста является эффективным мотивирующим фактором обретения навыков ответственного и уверенного выполнения принятых обязательств, умения корректировать сроки решения задач разной важности в обеспечение достижения назначенных целей.

Ключевые слова: самооценка; контрольные точки; квалиметрия развития; мотивация ответственности; результативность развития.

DIGITALIZATION OF SELF-CONTROL OF THE DEVELOPMENT INFORMATION WARFARE TECHNOLOGIES IN ADVANCED TRAINING

Alekseev Anatoly[1], Mikhalchuk Andrey[1], Musatenko Roman[2]
[1]Saint Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 194064, Russia
[2]VUNTS of the Navy «N.G. Kuznetsov Naval Academy»
17/1 Ushakovskaya Emb, St. Petersburg, 197045, Russia
e-mails: iapbgks@bk.ru, 335mav@mail.ru, rus-euro-roman@yandex.ru

Abstract: Among the systemic aspects of the concept and methodology of advanced learning, a special place belongs to the preparation and successful transition of the student to self-learning and self-control. Among the many factors in training in the direction of «Information Security» is the high dynamics and complexity of technological development, the growth of professional requirements. With the unconditional information, methodological and technological support of a university graduate, when forming a model of professional and career growth, with career guidance and goal setting, justification and digitalization of expected indicators and control points of self-development are mandatory when planning. Using the example of using the CMPC software package, it is shown that the combination of continuous monitoring of the results of self-study, project and publication activity, digitalization of self-control of professional and career growth is an effective motivating factor in acquiring the skills of responsible and confident fulfillment of commitments, the ability to adjust the timing of solving tasks of varying importance to ensure the achievement of assigned goals.

Keywords: self-assessment; control points; qualimetry of development; motivation of responsibility; effectiveness of development.

Среди системных аспектов концепции и методологии опережающего (развивающего) обучения и саморазвития, активно развиваемых в последнее время при совершенствовании системы подготовки ИТ-специалистов, при анализе прорывных технологий морских автоматизированных систем в защищенном исполнении [1, 2], особое место принадлежит подготовке и успешному переходу обучаемого к самообучению и самоконтролю (саморегулированию, личностной рефлексии).

При подготовке обучаемых по направлению «Информационная безопасность» среди множества обуславливающих факторов — высокая динамика и сложность технологического развития, роста профессиональных требований [1-5].

При безусловной информационно-методической и технологической поддержке выпускника ВУЗа, при формировании модели профессионального и карьерного роста, при профессиональном ориентировании и целеполагании обоснование и цифровизация ожидаемых показателей и контрольных точек саморазвития являются обязательными при планировании [6-7]. При этом, безусловным фактором реализации данного подхода следует считать автоматизацию процессов обоснования, цифровизации, своевременного планирования, дорожного картирования в «возрастной матрице 22*25*33*40*50*60» [8-12].

Одним из эффективных средств реализации при этом следует считать программный комплекс цифрового мониторинга, прогнозирования и контроля (ПК «ЦМПК») успешности реализации спланированного комплекса организационно-технических решений (КОТР) [13], который разработан для интерактивной цифровизации, визуализации и наблюдения, прогнозирования и контроля успешности реализации (возможности выполнения с заданным качеством) КОТР в заданный для него срок. ПК «ЦМПК» основан на интерактивной актуализации данных по реализации каждого из решений, адаптивном прогнозировании успешности их реализации на заданный для КОТР срок, а также на агрегировании прогнозных оценок в единый показатель успешности и его контроль для всего КОТР с соответствующей визуализацией и мониторингом.

ПК «ЦМПК» предназначен для подготовки и переподготовки специалистов организационно-технического мониторинга и управления созданием и эксплуатацией сложных объектов морской техники и инфраструктуры в судостроительной и других отраслях экономики [13]. Вместе с тем, это не исключает возможности его успешного использования для решения названных выше задач самоконтроля.

На ряде примеров использования программного комплекса «ЦМПК» для задач вариантного проектирования систем комплексной защиты информации показано, что сочетание непрерывного мониторинга результатов самообучения, проектной и публикационной активности, цифровизация самоконтроля профессионального и карьерного роста является эффективным мотивирующим фактором обретения навыков ответственного и уверенного выполнения принятых обязательств, умения корректировать сроки решения задач разной важности в обеспечение достижения назначенных целей.

Цифровой анализ достигнутых, ожидаемых и планируемых результатов в сопоставлении с подобными результатами конкурентов, в том числе в контексте минимизации рисков и оптимизации принимаемых решений, позволяет обучаемому количественно оценивать комплекс личных требований при заданных условиях модели динамичного саморазвития, профессиональной зрелости и карьерной успешности, контролировать достигаемые результаты по удобной, например, 50-бальной шкале и принимать своевременные корректирующие решения. Цифровая интерпретация фактических результатов позволяет молодым специалистам стимулировать самосознание, самодисциплину, самокритичность, самоуважение, что способствует обосновывать и решать самые распространенные «проблемы роста», низкой эффективности труда, методической неподготовленности, недостаточного владения методами обучения, неумения формулировать в ходе исследования проблемные вопросы, цели и задачи [14].

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б. Я., Касаткин В. В. Концептуальные основы совершенствования системы подготовки ИТ-специалистов // Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конф. Севастополь, 22-26.09.2020. С., 2020. С. 5-9.
2. Прорывные технологии морских автоматизированных систем в защищенном исполнении / Согонов С. А. [и др.] // Актуальные проблемы морской энергетики: материалы одиннадцатой международной научно-технической конференции. СПб. : СПбГМТУ, 2022. С. 69-77.
3. Смольников А. В., Алексеев А. В., Михальчук А. В. Методика подготовки и переподготовки кадров объектов морской инфраструктуры повышенного риска с использованием автоматизированных средств квалиметрического сравнения уровня технологического развития // Актуальные проблемы морской энергетики: Материалы третьей Всероссийской межотраслевой научно-технической конференции. СПб : Изд-во СПбГМТУ, 2014 С. 89-91.
4. Алексеев А. В., Мусатенко Р. И., Михальчук А. В. Методика оценки компетенций при подготовке и переподготовке кадров ВМФ // Региональная информатика (РИ-2014). XIV Санкт-Петербургская международная конференция. СПб. : СПОИСУ, 2014. С. 439-440.
5. Алексеев А. В., Мусатенко Р. И., Потехин В. С. Обоснование требований к системе объективной оценки компетенций специалистов // Актуальные проблемы морской энергетики: Материалы четвертой Всероссийской межотраслевой научно-технической конференции. Посвящается 125-летию профессора, д.т.н., заслуженного деятеля науки и техники В.А. Ваншейдта. СПб. : СПбГМТУ, 2015. С. 154-157.
6. Научные направления и научные школы обеспечения развития систем автоматизации объектов морской техники и морской инфраструктуры / Кузнецов В. В. [и др.] // Региональная информатика и информационная безопасность. Сборник трудов. Вып. 2. СПб. : СПОИСУ, 2016. С. 272-273.
7. Метод оценки компетентности и подготовленности экипажа судна / А Алексеев А. В. [и др.] // Региональная информатика (РИ-2016). Юбилейная XV Санкт-Петербургская международная конференция. Санкт-Петербург, 26-28 октября 2016 г. : Материалы конференции. СПб., 2016. С. 429-430.
8. Алексеев А. В., Михальчук А. В. От опережающего обучения к профессиональному и карьерному росту // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Санкт- Петербург, 26-28 октября 2022 г. : Материалы конференции. СПб. : СПОИСУ , 2022. С. 412-414.

9. Квалиметрическая оценка индекса компетентности специалиста и экипажа судна / Согонов С. А. [и др.] // International Confer-ence on Naval Architecture and Ocean Engineering. Collection of Papers. Труды Международной конференции по судостроению и океанотехнике: Сборник статей. СПб. : СПбГМТУ, 2016. С. 581-587.
10. Метод и технология автоматической оценки и мониторинга компетентности и подготовленности экипажа судна / Алексеев А. В. [и др.] // Корабельная энергетика: из прошлого в будущее: материалы Всероссийского межотраслевого научно-технического форума. СПб. : Изд-во СПбГМТУ, 2017. С. 334 — 338.
11. Алексеев А. В., Мусатенко Р. И. Принципы и технология квалиметрической оценки уровня подготовки командира корабля и специалистов // Актуальные проблемы профессиональной подготовки командиров кораблей и специалистов ВМФ. 30 мая 2017. СПб., ВИ ДПО ВУНЦ ВМФ «ВМА». С. 110-114.
12. Мусатенко Р. И., Алексеев А. В., Вербицкая К. М. Модель оценки компетенций обучающихся и ее использование при подготовке военных кадров ВМФ // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция Санкт-Петербург, 28-30 октября 2020 г. Материалы конференции. СПб. : . СПОИСУ, 2020. С. 182-184.
13. Алексеев А. В., Михальчук А. В. Цифровой мониторинг, прогнозирование и контроль успешности реализации комплекса организационно-технических решений (ЦМПК) //Свидетельство о государственной регистрации программ для ЭВМ (Реестр программ Федеральной службы по интеллектуальной собственности) № 2014613622, 01.04.2023 (06.02.2014).
14. Абульзанова-Славская К. А. Типология активности личности // Психологический журнал. 1985. Т. 6. № 5. С. 3-18.

УДК 629.12, 65.011, 681.518

ИНФОРМАЦИОННАЯ ЖИВУЧЕСТЬ УПРАВЛЕНИЯ: ТЕОРИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОГО ПРЕВОСХОДСТВА

Алексеев Анатолий Владимирович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 194064, Россия
e-mail: iapbgks@bk.ru

Аннотация. Рассмотрены теоретические и практические аспекты решения системной проблемы обеспечения информационного превосходства в управлении на базе технологических решений максимизации информационной живучести управления (ИЖУ) типовых объектов морской техники и морской инфраструктуры (ОМТИ). В качестве основных факторов модели ИЖУ ОМТИ приняты такие их свойства, как оперативность, достоверность, устойчивость, скрытность, непрерывность, ресурсоемкость с соответствующими частными показателями качества типа работное время решения комплекса функциональных задач, адекватность используемых данных, надежность, конфиденциальность, доступность, целостность, киберустойчивость, рефлексивность управления, имитоскрытность, эргогномичность. Показано, что обеспечение ИЖУ ОМТИ в условиях интенсивного информационно-технологического развития является сложнейшей задачей целеполагания, роботизированного управления с использованием высокоинтеллектуальных баз данных и знаний, технологий полимодельного мониторинга, анализа, синтеза и оптимизации управленческих решений с мониторингом контроля их реализации, адаптивной корректировки, верификации и валидного контроля.

Ключевые слова: целеполагание; информационное превосходство; информационная живучесть управления; жизненный цикл управления; валидный контроль.

INFORMATION SURVIVABILITY OF MANAGEMENT: THEORY AND PRACTICE OF ENSURING INFORMATION SUPERIORITY

Alekseev Anatoly Vladimirovich
Saint Petersburg State Maritime Technical University
3 Lotsmanskaya St, St. Petersburg, 194064, Russia
e-mail: iapbgks@bk.ru

Abstract. The theoretical and practical aspects of solving the systemic problem of ensuring information superiority in management on the basis of technological solutions for maximizing the information survivability of management (IU) of typical objects of marine equipment and marine infrastructure (OMTI) are considered. Such properties as efficiency, reliability, stability, secrecy, continuity, resource intensity with corresponding particular quality indicators such as working time for solving a set of functional tasks, adequacy of the data used, reliability, confidentiality, accessibility, integrity, cyber stability, reflexivity of management, imitokrytost, ergognomicity are accepted as the main factors of the OMTI IJU model. It is shown that the provision of OMTI IU in conditions of intensive information technology development is the most difficult task of goal-setting, robotic management using highly intelligent databases and knowledge, technologies of polymodel monitoring, analysis, synthesis and optimization of management decisions with monitoring of their implementation, adaptive adjustment, verification and valid control.

Keywords: goal setting; information superiority; information survivability of management; management lifecycle; valid control.

Развитие современных сложных организационно-технических систем (ОТС) в условиях интенсивного развития информационных технологий, включая ОМТИ, обостряет проблему их функциональной устойчивости и живучести ОТС [1-17], а в условиях расширения спектра информационных вторжений и информационного противоборства — к информационной устойчивости и ИЖУ ОТС в целом.

Введенное в 2019 г. [18] и развитое в ряде последующих исследований [19-22] понятие ИЖУ определяет способность ОТС сохранять работоспособность и заданную функциональную эффективность при информационном воздействии н вторжении в ОТС с нанесением ей соответствующего информационного ущерба. В отличие от традиционного понятия функциональной устойчивости ОТС, как способности сохранять свое состояние при влиянии внешних воздействий, предусматривает анализ и учет возможности структурной динамики и деградации элементов системы при одновременном выполнении ОТС ряда из заданных функций, в том числе с ограниченным качеством и эффективностью.

Под ИЖУ ОТС предложено понимать ее свойство сохранять во времени в установленных пределах функциональности (проектного качества, эффективности эксплуатации) способность выполнять заданные функции в заранее неопределенных динамически изменяющихся условиях при целенаправленном воздействии конкурента (противника, нарушителя регламентов информационного взаимодействия) на подсистему или ее отдельные элементы ОТС, в первую очередь, системы управления. Следует отметить, что это свойство имеет особо важное системное значение, агрегируя такие свойства, как надежность, адаптивность, робастность, отказоустойчивость, эффективность, восстанавливаемость и другие. Модель количественного оценивания ИЖ ОТС в значительной степени определяется сложностью ее организации, а по существу, безальтернативным методом следует считать квалиметрический. Ключевым признаком определения сущности свойства ИЖ является вид деструктивного воздействия, относительно которого определяется это свойство, их совокупность и соответствующая их факторная значимость для достижения целевых показателей ОТС.

Свойство ИЖ проявляется только в условиях неблагоприятных объективных и субъективных воздействий со стороны окружающей среды. Неблагоприятные воздействия могут иметь различную природу, что, в свою очередь, предполагает дифференциацию реакций ОТС на возникающую ситуацию. Так к воздействиям одного класса ОТС может оказаться индифферентной, а к другим более или менее критичной. Следует отметить невозможность определять ИЖ ОТС относительно неопределенных деструктивных воздействий. Оценивание показателей ИЖ и синтез структур обладающей ИЖ ОТС может осуществляться только по отношению к конкретному воздействию со стороны агрессивной внешней среды.

Рассмотрены теоретические и практические аспекты решения системной проблемы обеспечения информационного превосходства по критерию ИЖЗ ОТС на базе технологических решений максимизации информационной живучести управления (ИЖУ) типовых объектов морской техники и морской инфраструктуры (ОМТИ). В качестве основных факторов ИЖУ ОМТИ приняты такие их свойства, как оперативность, достоверность, скрытность, функциональная устойчивость, непрерывность, ресурсоемкость с соответствующими частными показателями качества типа работное время решения комплекса функциональных задач, адекватность используемых данных, информационная защищенность ресурсов и информационно-коммуникационных систем, адаптируемость, непрерывность функционирования.

Показано, что обеспечение ИЖУ ОТС, включая ОМТИ, в условиях интенсивного информационно-технологического развития является сложнейшей задачей целеполагания, роботизированного управления с использованием высокоинтеллектуальных баз данных и знаний, технологий полимодельного мониторинга, анализа, синтеза и оптимизации управленческих решений с мониторингом контроля их реализации, адаптивной корректировки и валидного контроля.

В этом контексте одной из сложнейших системных задач исследования теоретических и практических аспектов обеспечения ИЖ ОТС и информационного превосходства в целом является разработка модели и методологии результативного и эффективного управления ею [23-30]. Недооценка названных аспектов может приводить к ошибкам системного управления с соответствующими информационными рисками метауровня, цена которых существенно выше.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 27.002-2015. Надежность в технике. Термины и определения. М. : Стандартинформ, 2016. 30 с.
2. Бондаренко Д. Л., Жбанов И. Л. Анализ существующих подходов к трактовке понятия «живучесть» информационно-управляющей подсистемы асу специального назначения // Актуальные вопросы технических наук: материалы IV Междунар. науч. конф. К., 2017. С. 100-104.
3. Козлов М. В., Малашенко Ю. Е., Рогожин. В. С. Моделирование живучести систем энергетики: методология, модель, реализация.: ВЦ АН СССР, 1986. 58 с.
4. Двоеглазов Д. М. Живучесть и устойчивость предприятий сложной структуры в условиях воздействия внешних рисков, алгоритмы управления и модели адаптации рисков [Электронный ресурс] // НАУКОВЕДЕНИЕ. Технические науки. 2015. Том 7. №1(январь-февраль).URL: http://naukovedenie.ru/PDF/72TVN115.pdf (дата обращения 26.07.2023).
5. Словарь по кибернетике / под ред. В.С. Механевича. Киев : УСЭ, 1989. 751 с.
6. Беликов А. И. Общий случай оценки структурной живучести многополосных сетей военной связи. 1989.
7. Крылов А. Н. Собрание трудов. Теория корабля. Ч. 1. М.; Л. : АН СССР, 1948. Т. 9.
8. Иванов В. Л., Ширенко А. П., Доможиров В. Т., Семенихин В. К. Основы живучести военно-космических сил. Ч. 1. Проблемы, модели, информационное обеспечение. М.: МО СССР, 1991.
9. Черкесов Г. Н. Методы и модели оценки живучести сложных систем // Активная защита от отказов микропроцессорных вычислительных систем. М.: Знание, 1987.
10. Информационные технологии в судостроении: существующие системы, сферы и возможности их использования [Электронный ресурс] URL: https://uchimsya.com/a/qC363Pr9 (дата обращения 24.05.2023).
11. Анфилатов В. С., Емельянов А. А., Кукушкин А. А. Системный анализ в управлении: учебное пособие. М. : Финансы и статистика, 2002.368 с.
12. Бляхман Л. С. Основы функционального и антикризисного менеджмента: учебное пособие. СПб., 1999. 380 с.
13. Словарь по кибернетике / Под ред. В.М. Глушкова. Киев: Укр. сов. энциклопедии, 1979. 623 с.

14. Горшков В. В. Логико-вероятностный метод расчета живучести сложных систем. Кибернетика АН УССР.1982. № 1. С. 104-107.
15. Волик Б. Г., Рябинин Й. А. Эффективность, надежность и живучесть управляющих систем // Автоматика и телемеханика. 1984. № 12.
16. Надежность, в технических системах. Справочник / Под ред. И. Н. Ушакова. М. : Радио и связь, 1985. 606 с.
17. Рябинин И. А., Парфенов Ю. Н. Надежность и эффективность структуры сложных технических систем // Основные вопросы теории и практики надежности. Минск: Наука и техника, 1982. С. 25-40.
18. Алексеев А. В., Кириллов Н. П. Информационная устойчивость морских радиоэлектронных систем в условиях широкомасштабной информационной войны // Наука и техника: Вопросы истории и теории. Тезисы 18 конф. СПб отд-я Нац. комитета по истории и философии науки и техники. Вып. 13. СПб.: СПФИИЕТ РАН, 1997. С.13-14.
19. Алексеев А.В., Кириллов Н. П. Информационная устойчивость систем морской разведки в условиях широкомасштабной информационной борьбы // Разведка и радиоэлектронная борьба. Тез. докл. МВНС. СПб.: В/ч 48252, 1999. С. 65-67.
20. Алексеев А.В. Информационная живучесть судна: понятие, проблемы, технологии / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7. СПб. : СПОИСУ, 2019. С. 345 — 348.
21. Алексеев А. В., Смольников А. В., Сус Г. Н., Ушакова Н. П. Когнитивные технологии системы поддержки принятия решений и управления борьбой за живучесть корабля, судна //Системы управления и обработки информации: научн.-техн. сб. СПб., 2019. Вып. 3(46). С. 18-27.
22. Обоснование системы критериев оценки информационной живучести судна / Алексеев А. В. [и др.] // Региональная информатика и информационная безопасность. Сборник трудов. Вып. 7. СПб. : СПОИСУ, 2019. С. 353-358.
23. Система критериев оценки информационной живучести судна / Алексеев А. В. [и др.] // Информационная безопасность регионов России (ИБРР-2019). СПб., 2019. С. 329-330.
24. Бобрович В. Ю., Алексеев А. В., Антипов В. В., Смольников А. В. Информационная живучесть корабля: угрозы, модель, системные требования, пути реализации // Информационная безопасность регионов России (ИБРР-2021). СПб., 2021. С. 265-267.
25. Алексеев А. В. Модель и программный комплекс цифровой трансформации кибербезопасности // Вопросы обеспечения безопасности в киберпространстве: материалы Всероссийской НТК. Махачкала: ДГТУ, 2022. С. 251-255.
26. Корнева Ю. В., Алексеев А. В. Информационная живучесть тактической группы кораблей. СПбГМТУ : ВКР, 2023. 75 с.

УДК 629.12, 65.011, 681.518

ЦИФРОВОЙ ДВОЙНИК СИСТЕМ АВТОМАТИЗАЦИИ ПРОЦЕССОВ БОРЬБЫ ЗА ИНФОРМАЦИОННУЮ ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА

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

Аннотация. В развитие теоретических и практических аспектов системной проблемы обеспечения информационного превосходства в управлении решена прикладная задача обоснования структуры и алгоритма функционирования цифрового двойника (ЦД) систем автоматизации процессов борьбы за информационную живучесть корабля, судна (САП БИЖКС). Показано, что перспективным направлением развития САП БИЖКС следует считать интеграцию технологических решений систем интеллектуальной поддержки решений и управления на базе программных комплексов типа «СПРУ» и «ЦД СКЗИ», что обеспечивает информационное превосходство в управлении более 12 % за счет повышения его оперативности, устойчивости и достоверности принимаемых решений.

Ключевые слова: информационная живучесть управления; информационное превосходство; технологическая интеграция; роботизация.

DIGITAL TWIN OF PROCESS AUTOMATION SYSTEMS FOR FIGHTING FOR INFORMATION SURVIVABILITY OF SHIP, PRODUCTION SAFETY MONITORING

Alekseev Anatoly, Antipov Vasily, Smolnikov Alexander
Institute for Automation of Struggle Pocess for the Survivability of the Ship»
101 Leninsky Av, St. Petersburg, 198262, Russia
e-mail: iapbgks@bk.ru

Abstract. In the development of theoretical and practical aspects of the system problem of ensuring information superiority in management, the applied task of justifying the structure and algorithm of the functioning of the digital twin (CD) of the automation systems of the processes of struggle for information survivability of a ship, vessel (SAP BIZhKS) was solved. It has been shown that integration of technological solutions of intelligent support systems for solutions and control based on software systems such as «SPRU» and «CD CIPF» should be considered a promising direction of SAP development, which ensures information superiority in management of more than 12% due to increasing its efficiency, stability and reliability of decisions made.

Keywords: information survivability of the control; information superiority; technological integration; robotization.

В развитие теоретических и практических аспектов системной проблемы обеспечения информационного превосходства в управлении [1, 2] особое место занимает проблема обеспечения функциональной устойчивости и живучести сложных организационно-технических систем [3-11]. В условиях интенсивного развития информационных технологий, расширения спектра информационных вторжений и информационного противоборства в управлении в целом, все большую актуальность приобретает проблема гарантированного обеспечения информационной живучести системного управления в целом (ИЖСУ) [12-20].

Понятие ИЖСУ предлагается интерпретировать как свойство системы управления сохранять во времени и в установленных пределах функциональных требований (проектного качества и заданной эффективности эксплуатации) способность выполнять свои функции в заранее неопределенных и динамически изменяющихся условиях под воздействием внешних и внутренних, объективных и субъективных факторов фиксированного состава. Как следует из определения, вводимая неопределенность условий, тем не менее, ограничена фиксируемым составом воздействующих факторов с соответствующими известными в науке и практике характерными параметрами. Это позволяет решать задачу количественных оценок на вариантном уровне с согласованием модельных параметров между Заказчиком и Проектантом.

Применительно к критическим системам, к числу которых в полной мере относятся системы автоматизации процессов борьбы за информационную живучесть корабля, судна, в этой связи возникает ряд задач, требующих как теоретического, так и прикладного неотложного решения. Именно применительно к САП БЖКС в докладе рассмотрена и приведено возможное эффективное решение прикладной задачи обоснования возможности и целесообразности использования, а также обоснования структуры и алгоритма функционирования сравнительно нового и интенсивно развивающегося технологического решения — цифровых двойников [21].

В результате выполненного вариантного квалиметрического анализа свойств и характеристик САП БЖКС с использованием накопленных прикладных данных и знаний [1, 2, 16, 19, 20-23], а также использования технологии и роботизированного проектного комплекса ЦД «ЦД СКЗИ» [24], ранее накопленная и непрерывно актуализируемая квалиметрическая база данных и знаний (КБДЗ) технологий и средств реализации САП БИЖКС типа «ПК МДО СИП ЛА-ГО» [22] и «СПРУ» [23] была адаптирована к формату ЦД в варианте «ЦД СКЗИ» [24]. Это позволило в формате ЦД создать в модуле «1.ЦП» так называемый цифровой паспорт САП БИЖКС и выполнить предусмотренный возможностями ЦД анализ корневой чувствительности агрегированного показателя качества (АПК) к изменению каждого из частных показателей качества. Анализ корневой чувствительности показал, что приоритетными для наращивания проектного качества и эффективности эксплуатации являются системные свойства САП БЖКС оперативности, устойчивости и достоверности принимаемых решений.

Выполненное вариантное исследовательское проектирование показало, что интеграция технологических решений систем интеллектуальной поддержки решений и управления на базе программных комплексов типа «СПРУ» с ЦД на базе робототехнических комплексов типа «ЦД СКЗИ» обеспечивает информационное превосходство в управлении более 12% за счет: повышения оперативности СПРУ путем прироста вариантности цифрового моделирования проектных решений и увеличения объема данных в КБДЗ; повышения устойчивости СПРУ путем повышения числа сценариев фактической обстановки при тренажерной их отработке; повышения достоверности принимаемых решений СПРУ путем расширения ряда альтернативных вариантов решений при выборе оптимального из них, повышения точности вводимых исходных данных, адекватности используемых данных, сопоставляемых в ЦД с соответствующими модельными данными; повышения информационной защищенности СПРУ в составе интегрированного решения «СПРУ&ЦД» путем распределения решаемых задач в СПРУ и ЦД; повышения робастности СПРУ путем дополнительных возможностей по адаптируемости ЦД к широкому спектру возможных деструктивных факторов и за счет ряда других преимуществ интегрального решения «СПРУ&ЦД».

Более того, показано, что имеет место «эффект системной нейтрализации» роста ресурсоемкости при интеграции СПРУ и ЦД, включая определенное снижение надежности функционирования, большим значением прироста системного качества, но при определенном ограничении типа допустимого значения увеличения ресурсных затрат СПРУ порядка 32 %, что позволяет рекомендовать развитие технологий ЦД по типу «калькуляторов СПРУ» [21]. Вместе с тем, этот сложный системный вопрос требует дополнительного дальнейшего исследования и уточнения границ рекомендаций.

СПИСОК ЛИТЕРАТУРЫ

1. Современные технологии автоматизации борьбы за живучесть корабля, судна: итоги работы авторского коллектива при написании монографии / А. В. Алексеев [и др.] // Региональная информатика (РИ-2022). XVIII Санкт-Петербургская международная конференция. СПб., 2022. С. 409-411. Бобрович В. Ю. [и др.] // Седьмая международная НРК «Имитационное и комплексное моделирование морской техники и морских транспортных систем (ИКМ МТМТС-2023)». М. : Перо, 2023. С. 10-14.
2. Крылов А. Н. Собрание трудов. Т. 9. Теория корабля. Ч. 1. М. ; Л.: АН СССР, 1948.
3. Словарь по кибернетике / Под ред. В. М. Глушкова. Киев: Гл., ред. Укр. сов. энциклопедии, 1979.
4. Рябинин И. А., Парфенов Ю. Н. Надежность и эффективность структуры сложных технических систем // Основные вопросы теории и практики надежности. Минск: Наука и техника, 1982. С. 25-40.
5. Волик Б. Г., Рябинин Й. А. Эффективность, надежность и живучесть управляющих систем // Автоматика и телемеханика. 1984. № 12. Надежность, в технических системах : справочник / Под ред. И. Н. Ушакова. М.: Радио и связь, 1985. 606 с.
6. Моделирование живучести систем энергетики: методология, модель, реализация / М. В. Козлов [и др.]. М.: ВЦ АН СССР, 1986.
7. Черкесов Г. Н. Методы и модели оценки живучести сложных систем // Активная защита от отказов микропроцессорных вычислительных систем. М.: Знание, 1987.116 с.
8. Беликов А. И. Общий случай оценки структурной живучести многополосных сетей военной связи. 1989. Вып. 1.
9. Информационные технологии в судостроении: существующие системы, сферы и возможности их использования. [Электронный ресурс] URL: https://uchimsya.com/a/qC363Pr9 (дата обращения 24.05.2023).
10. Иванов В. Л., Ширенко А. П., Доможиров В. Т., Семенихин В. К. Основы живучести военно-космических сил. Ч. 1. Проблемы, модели, информационное обеспечение. М.: МО СССР, 1991.
11. Алексеев А. В., Кириллов Н. П. Информационная устойчивость морских радиоэлектронных систем в условиях широкомасштабной информационной войны // Наука и техника: Вопросы истории и теории : тезисы 18 конф. СПб отд-я Нац. комитета по истории и философии науки и техники. Вып. 13. СПб: СПФИИЕТ РАН, 1997. С. 13-14.

12. Двоеглазов Д. М. Живучесть и устойчивость предприятий сложной структуры в условиях воздействия внешних рисков, алгоритмы управления и модели адаптации рисков // Интернет-журнал «НАУКОВЕДЕНИЕ». 2015. Т. 7, № 1.
13. Бондаренко Д. Л., Жбанов И. Л. Анализ существующих подходов к трактовке понятия «живучесть» информационно-управляющей подсистемы АСУ специального назначения // Актуальные вопросы технических наук, 2017. С. 100-104.
14. Алексеев А. В. Информационная живучесть судна: понятие, проблемы, технологии // Региональная информатика и информационная безопасность : сб.трудов. Вып. 7. СПб: СПОИСУ, 2019. С. 345–348.
15. Алексеев А. В., Смольников А. В., Сус Г. Н., Ушакова Н. П. Когнитивные технологии системы поддержки принятия решений и управления борьбой за живучесть корабля, судна // Системы управления и обработки информации : научн.-техн. сб. АО «Концерн «НПО «Аврора». СПб, 2019. Вып. 3(46). С. 18-27.
16. Обоснование системы критериев оценки информационной живучести судна / А. В. Алексеев [и др.] // Региональная информатика и информационная безопасность: сб. трудов. Вып. 7. СПб. : СПОИСУ, 2019. С. 353–358.
17. Система критериев оценки информационной живучести судна / А. В. Алексеев, В. В. Кузнецов, С. А. Согонов [и др.] // Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская Межрегиональная конференция. СПб., 2019. С. 329-330.
18. Бобрович В. Ю., Алексеев А. В., Антипов В. В., Смольников А. В. Информационная живучесть корабля: угрозы, модель, системные требования, пути реализации // Информационная безопасность регионов России (ИБРР-2021). СПб., 2021. С. 265-267.
19. Корнева Ю. В. Информационная живучесть тактической группы кораблей. СПбГМТУ: ВКР, 2023. 75 с.
20. Модель и технология цифровых двойников систем автоматизации судов / А. В. Алексеев [и др.] // Актуальные проблемы морской энергетики: материалы одиннадцатой международной научно-технической конференции. СПб.: Изд-во СПбГМТУ, 2023. С. 12-20.
21. Программный комплекс Макетного действующего образца Системы информационной поддержки судоводителей при обеспечении безопасности эксплуатации в части грузовых операций, локализации аварийных ситуаций, аварий и борьбы за живучесть морских объектов повышенного риска (ПК МДО СИП ЛА-ГО о3): свидетельство о гос. регистрации программ для ЭВМ № 2014614620, 29.04.2014.
22. Программный комплекс системной поддержки принятия решений и управления (СППРУ): свидетельство о гос. регистрации программ для ЭВМ № 2023.5.19. 2023616019_2023.3.14.
23. Цифровой двойник системы комплексной защиты информации в инвариантном исполнении (ЦД СКЗИ): свидетельство о гос. регистрации программ для ЭВМ № 2023619940, 2023.5.19.

УДК 57.08

КОНТРОЛЬ ЗА ПРОЯВЛЕНИЕМ ДЕПРЕССИВНОГО СОСТОЯНИЯ У СПЕЦИАЛИСТОВ МОРСКОГО И РЕЧНОГО ФЛОТА, КАК НАПРАВЛЕНИЕ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ СУДОВОЖДЕНИЯ

Артемов Станислав Игоревич[1], Алексеев Сергей Алексеевич[2], Рябков Яков Игоревич[3]
[1]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул.,5, Санкт-Петербург, 197376, Россия
[2] Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
[3]Военно-космическая академия имени А.Ф. Можайского
Ждановская ул., 13, Санкт-Петербург, 197198, Россия
e-mails: pushokcheck@yandex.ru, ksgati@yandex.ru, yakovrt@mail.ru

Аннотация. В статье рассмотрен метод, выполненный в безопасном исполнении, по анализу многоканальной электроэнцефалограммы, позволяющий фиксировать связь динамики параметров распределения амплитуд с психофизиологическими свойствами испытуемых. В основу метода положена информационная символьно-динамическая модель многоканальной электроэнцефалограммы и соответствующая модели модификация нелинейного структурно-лингвистического метода анализа сигналов. Полученные результаты позволяют сделать вывод о влиянии физиологического состояния испытуемого, его депрессивного состояния на параметры динамики распределения амплитуд в многоканальном сигнале электроэнцефалограммы.

Ключевые слова: обработка сигналов; восприятия; психофизиологические реакции мозга; обработка электроэнцефалограмм; интерфейс мозг-компьютер; нелинейный анализ сигналов; энтропия.

CONTROL OVER THE MANIFESTATION OF A DEPRESSIVE STATE AMONG SPECIALISTS OF THE MARINE AND RIVER FLEET, AS A DIRECTION FOR IMPROVING THE SAFETY OF NAVIGATION

Artemov Stanislav[1], Alekseev Sergey[2], Ryabkov Yakov[3]
[1]St. Petersburg State Electrotechnical University «LETI» named after V.I. Ulyanov (Lenin)
5 Professor Popov's St, St. Petersburg, 197376, Russia
[2]Federal University of the Sea and River Fleet named after Admiral S.O. Makarov,
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
[3]Military Space Academy named after A.F. Mozhaisky
13 Zhdanovskaya St, St. Petersburg, 197198, Russia
e-mails: pushokcheck@yandex.ru, ksgati@yandex.ru, yakovrt@mail.ru

Abstract. The article considers a method performed in a safe execution, based on the analysis of a multichannel electroencephalogram, which allows to fix the relationship of the dynamics of the parameters of the amplitude distribution with the psychophysiological properties of the subjects. The method is based on an informational symbolic-dynamic model of a multichannel electroencephalogram and a modification of the nonlinear structural-linguistic method of signal analysis corresponding to the model. The obtained results allow us to conclude about the influence of the physiological state of the subject, his depressive state on the parameters of the dynamics of the distribution of amplitudes in the multichannel signal of the electroencephalogram.

Keywords: automation of management; organizational management; scientific and production association; social organizational and technical system.

Важным требованием для обеспечения безопасности эксплуатации транспортных средств и техники морского и речного флота является предрейсовый медицинский контроль и осмотр физического состояния участвующих в нем специалистов. При этом в методических рекомендациях не представлены методы, позволяющие осуществлять объективный контроль последствий нарушения режима труда и отдыха, таких как утомление и депрессивные состояния. Известно, что традиционные линейные методы анализа ЭЭГ недостаточно эффективны при обнаружении депрессивных состояний водителей транспортных средств[1-4].

По данным таких известных исследователей, таких как П. Линдсей (1974) и Саид Саней (1990) и многих других, при предъявлении стимула сигнал от рецепторов сигнал проходит последовательную обработку в различных областях мозга и излучается на фоне сигнала, известного, как «спонтанная активность». Спонтанная активность и аддитивность сигнала, регистрируемого отведениями электроэнцефалографа увеличивают соотношение сигнал-шум при обнаружении вызванного потенциала. Для обнаружения волны вызванного потенциала, соответствующего предъявляемому стимулу, обычно используется накопление синхронных относительно предъявления стимула временных интервалов сигнала электроэнцефалограммы (ЭЭГ). Сигнал вызванного потенциала, синхронизированного с предъявлением стимула, фиксируется прибором снятия ЭЭГ как суперпозиция с сигналами «спонтанной активности». Этим объясняется низкие значения отношения сигнал-шум при обнаружении волны вызванного потенциала. В настоящем исследовании предлагается использование информационной символьно-динамической модели для обработки электрофизиологических сигналов мозга без подавления «спонтанной активности» накоплением.

Целью исследования, представленного в статье метода контроля и обнаружения последствий нарушения режима труда и отдыха в виде утомления и депрессивного состояния лиц, привлеченных к управлению средствами морского и речного флота. Для достижения поставленной цели была разработана модель контроля маркеров утомляемости и депрессивного состояния через оценку сигнала электроэнцефалограммы (ЭЭГ), как проекции сигналов пространственно-временной обработки поступающего потока сенсорной нейронной активности на точки установления электродов съёма гальванических потенциалов для обоснования выбора метода выделения паттернов ЭЭГ (паттерн является качественной характеристикой ЭЭГ, отражающей функциональное состояние головного мозга). Разработана методика обнаружения маркеров утомляемости и депрессивного состояния, базирующуюся на оценке изменений элементного состава множества паттернов, выделяемых в сигнале ЭЭГ и алгоритм автоматизации и интеллектуализации процесса обнаружения маркеров утомляемости и депрессивного состояния в сигнале ЭЭГ, позволяющий автоматизировать выделение множества специфических паттернов, представленных амплитудно-временными структурами сигнала и выполнена экспериментальная проверка разработанных инструментов обработки и анализа сигналов ЭЭГ для выделения маркеров депрессивного состояния специалистов морского и речного флота.

Метод обнаружения моментов восприятия человеком визуальных стимулов, базируется на оценке изменений элементного состава множества паттернов, выделяемых путём построения амплитудно-временных конструкций, выделяемых в сигнале ЭЭГ. Теория и практика препроцессинга сигналов ЭЭГ и последующего анализа с применением информационного подхода получили название структурно-лингвистического анализа сигналов (СЛАС).

В основе СЛАС положено выделение из сигнала повторяющихся конструкций с идентичными амплитудно-временными отношениями последовательностей максимальных и минимальный значений функции сигнала на протяжении фрагмента анализа выделенного ЭЭГ — паттернов. Суть метода основывается на информационной символьно-динамической модели, как модификации метода структурно-лингвистического анализа сигналов (СЛАС). В соответствии с данным методом производится поиск в сигнале фазоамплитудных последовательностей — символов и формирование для анализируемого сигнала множества символов — алфавита. Принцип преобразования сигнала ЭЭГ в последовательность особых точек носит нелинейный характер и включает автосегментацию, что делает его устойчивым к шумам и изменению масштабов пространства, времени и амплитуды сигнала.

Для выполнения экспериментальной проверки разработан алгоритм высокопроизводительного структурно-лингвистического анализа сигналов ЭЭГ. Выполнена экспериментальная проверка полученного инструментального комплекса с использованием сигналов ЭЭГ. Получено, что при использовании таких вычисляемых параметров сигнала, как количество символов (размер алфавита) и энтропия Шеннона была достигнута чувствительность обнаружения и контроля депрессивных состояний, превышающая 95%.

Разработана модель многоканального сигнала электроэнцефалограммы, отличающаяся от известных тем, что в ней распределения электрической активности по поверхности головы испытуемого представляются как информационные символы. Анализом временной последовательности (динамики) таких символов достигается возможность классификации интенсивности деятельности головного мозга испытуемого.

Разработана методика обнаружения маркеров депрессивного состояния, базирующаяся на оценке изменений элементного состава множества паттернов, выделяемых в сигнале ЭЭГ.

Разработан алгоритм автоматизации и интеллектуализации процесса обнаружения маркеров утомляемости и депрессивного состояния в сигнале ЭЭГ, позволяющий автоматизировать выделение множества специфических паттернов, представленных амплитудно-временными структурами сигнала, и отличающийся от

традиционных тем, что позволяет выполнять анализ сигналов в соответствии с информационной символьно-динамической моделью.

Выполнена экспериментальная проверка разработанных инструментов обработки и анализа сигналов ЭЭГ для выделения маркеров депрессивного состояния. Показано, что предложенный метод может быть использован для обнаружения маркеров депрессивных состояний у сотрудников морского и речного флота. Чувствительность метода составляет не менее 95 %.

СПИСОК ЛИТЕРАТУРЫ

1. Артемов С. И., Алексеев С.А., Рябков Я. И. Анализ модели электроэнцефалограммы специалистов морского и речного флота как суперпозиции излучений множества источников // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. СПб. : СПОИСУ, 2022. 626 с.
2. Артемов С. И. Инвариантное кодирование сигналов электроэнцефалограммы для исследования ее информационных характеристик. // Прикладные проблемы безопасности технических и биотехнических систем. 2019.С. 37-41
3. Артемов С. И. Информационная модель электрофизиологических сигналов мозга // Universum: Химия и биология: электрон. Научн. Журн. 2015. № 12 (19). URL: http//7universum.com/ru/nature/archieve/item/2809 (дата обращения: 26.07.2023).
4. Артемов С. И. Многоканальная обработка данных электроэнцефалограммы на основе структурно-лингвистического анализа сигналов // Актуальные проблемы естественных и математических наук в России и за рубежом. Новосибирск, 2015. № 2. С. 100-103.

УДК 681.3.06

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИНФОРМАЦИОННОЙ ЖИВУЧЕСТИ ПРОГРАММНЫХ СИСТЕМ КЛАССА «EAM»

Бондаренко Андрей Игоревич, Головизнина Ольга Игоревна, Алексеев Анатолий Владимирович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 194064, Россия
e-mails: bear555.ru@gmail.com, golovizninaolga92@yandex.ru, 25st1@bk.ru

Аннотация. В докладе рассматривается и анализируется информационная живучесть технологий и программных систем класса EAM, обеспечивающих автоматизацию процессов учета, технического обслуживания и ремонта основных фондов предприятия. Квалиметрическое ранжирование технологий и EAM — систем, в том числе с учетом защищенности от ошибок операторов, обусловленных функциональной и алгоритмической сложностью использования, позволило обоснованно рекомендовать к внедрению в морских проектно-конструкторских бюро, на судостроительных и судоремонтных предприятиях программное средство «NERPA» при конкурентном превосходстве в 4,5% и перспективности развития 95,7%.

Ключевые слова: информационная устойчивость; база данных и знаний; актуализация; ранжирование; фактор; превосходство.

COMPARATIVE ANALYSIS OF INFORMATION VITALITY «EAM» CLASS SOFTWARE SYSTEMS

Bondarenko Andrey, Goloviznina Olga, Alekseev Anatoly
St. Petersburg State Marine Technical University,
3 Lotsmanskaya St, St. Petersburg, 194064, Russia
e-mails: bear555.ru@gmail.com, golovizninaolga92@yandex.ru, 25st1@bk.ru

Abstract. The report examines and analyzes the information survivability of technologies and software systems of the EAM class that provide automation of accounting processes, maintenance and repair of fixed assets of the enterprise. Qualimetric ranking of technologies and EAM systems, including taking into account the protection from operator errors caused by the functional and algorithmic complexity of use, allowed us to reasonably recommend the NERPA software tool for implementation in marine design bureaus, shipbuilding and ship repair enterprises with a competitive advantage of 4.5% and a development prospect of 95,7 %.

Keywords: information stability; database and knowledge; updating; ranking; factor; excellence.

Развитие судостроения и его конкурентоспособность связаны с целым рядом факторов объективного и субъективного характера, включая качество информационно защищенном исполнении (ЗИ) программных средств (ПС) и их комплексов (ПК) [1].

Среди факторов ЗИ, как известно, обязательно следует учитывать защиту используемых ПС и ПК от возможных (случайных), а также преднамеренных (в случае инсайдеров) ошибок операторов в разных вариантах. И чем выше функциональная сложность ПС и ПК, тем большее значение имеют факторы деструктивного воздействия, неустойчивости функционирования и ограниченной информационной живучести [2] наряду с другими, а, следовательно, требует внимания и контроля при выборе и внедрении соответствующих ПС и ПК в производство.

Несколько классов ИТ и реализующих их ПС и ПК интегрированы в ИТ АСУП (автоматизированные система управления предприятием), предназначенные для решения задач планирования и управления различными видами деятельности предприятия [2], включая задачи и технологии: управления цепочками поставок (SCM); планирования ресурсов предприятия (ERP); планирования производства (MRP, MRP II).

Одной из таких ИТ в комплексе АСУП является система EAM (Enterprise Asset Management System) — логическое развитие компьютерных систем управления ремонтами, существующих уже более 20 лет. EAM-системы предназначены для автоматизации бизнес-процессов учета, технического обслуживания и ремонта основных фондов, обеспечивая комплексную и согласованную деятельность организации, целью которой является оптимальное («идеальное») управление физическими активами и режимами их работы, рисками и расходами в процессе жизненного цикла для достижения и выполнения стратегических планов организации. EAM дает возможность уменьшения простоя оборудования, сокращения затрат на техобслуживание, ремонты и материально-техническое снабжение [3].

Методология EAM дает возможность за счет применения ИТ, не прибегая к закупкам нового оборудования, увеличить производственную мощность предприятия, согласованно управляя такими процессами как: ТОиР — техническое обслуживание и ремонт; МТС — материально-техническое снабжение; ТОиР — управление складскими запасами (запчасти для); прикладное управление финансами, персоналом и документами. При этом, функциями EAM-системы являются:

1. Формирование целостной базы оборудования и нормативно-справочной информации по его обслуживанию.
2. Составление плана мероприятий по техническому обслуживанию и ремонтам оборудования (ТОРО).
3. Организация заявочной компании.
4. Наблюдение за процессами обслуживания и ремонта оборудования.
5. Контроль реальных затрат в разрезе объектов и мероприятий.
6. Фиксация главных технологических подходов в работе оборудования (выходы из строя, простои).
7. Прорабатывание требующихся мероприятий по обслуживанию на базе данных АСУТП.
8. Обеспечение передачи необходимой информации в ERP.
9. Проведение оценки информации по ТОРО и организация корпоративной отчетности.

К числу положительных сторон EAM в составе АСУП относятся:

1. Сокращение трудоемкости процессов управления главными фондами.
2. Увеличение показателя готовности оборудования, повышение срока его работы.
3. Обеспечение совместного планирования ремонтов оборудования и уменьшение времени их проведения.
4. Увеличение продуктивности работы ремонтного персонала.
5. Сокращение объема складских запасов ТМЦ и оптимизация расходов на выполнение заявочной компании.
6. Способность оценить расходы и эффективность деятельности подразделений по обеспечению работоспособности оборудования.
7. Методология управления, с помощью которой можно повысить производственную мощность предприятия используя только ИТ, без приобретения нового оборудования.

В настоящее время система EAM — это полностью интегрированное программное решение, созданное для контроля за каждодневной эксплуатационной деятельностью капиталоемкого предприятия и сопровождения жизненного цикла его основных активов и фондов. Использование EAM-систем позволяет сократить время простаивания, уменьшаются затраты на техобслуживание оборудования, и эксплуатация базовых средств становится наиболее эффективной [4].

В результате квалиметрического исследования ИТ класса EAM по методологии применительно к условиям управления ремонтами и техническим обслуживанием инфраструктурных объектов была актуализирована ранее сформированная база данных и знаний (БДЗ) на интервале актуализации 1.09.2022-15.05.2023 с использованием технологии и робототехнического проектного комплекса (РПК) «АСОР-22.4» с учетом специфики объекта информатизации и сложившейся геополитической ситуации.

При этом, рассматривались EAM — системы, распространенные как на российском рынке, так и на зарубежном в контексте импортозамещения наиболее совершенных ПС и их ПК. Также при актуализации БДЗ учитывалась информация российской прессы, печатные материалы фирм–разработчиков и отзывы пользователей. Критериями выбора ПС и ПК из общего числа программного обеспечения (далее ПО) класса EAM – систем стали: функциональные возможности и свойства, эксплуатационные показатели, интегрируемость с ПС и ПК в составе АСУ и другими ИТ, ресурсные показатели и обеспеченность, эргономические показатели, популярность, отзывы, массовость на рынке, полнота информации о ПО.

Однако, наиболее значимым с индексом критериальной значимости 0,15 при общем числе критериев 12 был определен Обобщенный показатель качества информационной защищенности контента ПС по данным сертификации (ОУС). Именно это позволило с учетом функциональной и алгоритмической сложности альтернативных вариантов ПС, ПК и соответствующей важности фактора информационной живучести и устойчивости, учесть одно из важнейших требований к современным ИТ и реализующим их ПС по обеспечению конфиденциальности данных (учитывает факторы качества защиты корпоративной, государственной и т. п. тайны), доступности (факторы разграничения доступа, надежности и информационной живучести, устойчивости функционирования, киберзащищенности), целостности (факторы возможности модификации данных), что в целом определяет интегральный уровень информационной защищенности (информационной безопасности (ИБ) и ЗИ ПС).

Сравнительный анализ был выполнен применительно к судостроительным, судоремонтным предприятиям и проектно-конструкторским бюро с целью решения следующих основных задач: оптимизации управления складскими процессами; сокращения издержек; переход к дистанционному управлению.

В ходе ранжирования конкурентными вариантами ИТ класса EAM (ТОП – 5) было принято целесообразным по методологии ранжирования считать: 1. «NERPA» [5]. У данного ПС агрегированный (сводный) показатель качества по методике квалиметрического SWOT-анализа (QSWOT) Q=6,32; коэффициент конкурентного преимущества — КП=1,045; коэффициент перспективности развития — ПР=0,957. 2. «Галактика». Q=6,05; КП=1,000; ПР=1,000. 3. «IBM Maximo». Q=6,19; КП=1,023; ПР=0,978. 4. «CalemEAM». Q=6,40; КП=1,57; ПР=0,946. 5. «InforEAM». Q=5,69; КП=0,940; ПР=1,064.

В результате актуализации БДЗ ПС в классе EAM и актуализации соответствующего ряда ТОП-5 лидирующее средство «NERPA» при конкурентном превосходстве в 4,5% и перспективности развития 95,7% может быть обоснованно рекомендовано к внедрению в морских проектно-конструкторских бюро, на судостроительных и судоремонтных предприятиях, что позволит повысить эффективность управления в целом жизненным циклом продукции и услуг.

СПИСОК ЛИТЕРАТУРЫ

1. Информационные технологии в судостроении: существующие системы, сферы и возможности их использования [Электронный ресурс]. URL: https://uchimsya.com/a/qC363Pr9 (дата обращения 24.05.2023).
2. Алексеев А.В. Информационные технологии в жизненном цикле морской техники: курс лекций. СПб. : СПбГМТУ, 2023.
3. Информационные системы управления основными фондами (EAM — системы) [Электронный ресурс]. URL: http://www.systematic.ru/informatsionnye_sistemy.html (дата обращения 25.05.2023).
4. Анализ рынка EAM-систем. [Электронный ресурс].URL: http://www.galaktika.ru/eam/analiz-rynka-eam-sistem.html (дата обращения 25.05.2023).
5. NERPA EAM — система управления основными фондами и активами предприятия [Электронный ресурс]. URL: https://www.novosoft.ru/nerpa/eam (дата обращения 29.03.2023).

УДК 004.514.6

ОЦЕНКА ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА «MRP» В ЖИЗНЕННОМ ЦИКЛЕ ОБЪЕКТА МОРСКОЙ ТЕХНИКИ И ИХ ПРИМЕНЕНИЕ

Головизнина Ольга Игоревна, Родоманова Кристина Сергеевна, Алексеев Анатолий Владимирович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 194064, Россия
e-mail: golovizninaolga92@yandex.ru, kristina.rodomanova@mail.ru, 25st1@bk.ru

Аннотация. В докладе рассматриваются MRP–системы, наиболее подходящие для жизненного цикла объекта морской техники. Квалиметрическое ранжирование лучших MRP – систем и их практическое освоение.

Ключевые слова: MRP; информационные технологии; жизненный цикл; ранжирование.

ASSESSMENT OF THE USE OF MRP CLASS INFORMATION TECHNOLOGIES IN THE LIFE CYCLE OF A MARINE EQUIPMENT OBJECT AND THEIR APPLICATION

Goloviznina Olga, Rodomanova Kristina, Alekseev Anatoly
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 194064, Russia
e-mail: golovizninaolga92@yandex.ru, kristina.rodomanova@mail.ru, 25st1@bk.ru

Abstract. The article considers MRP-systems most suitable for the life cycle of marine equipment. Qualimetric ranking of the best MRP-systems and their practical mastering.

Keywords: MRP; information technology; life cycle; ranking.

Современная MRP — это тесно интегрированная замкнутая система, которая охватывает все предприятие. Она отслеживает все операции и постоянно взаимодействует с системами планирования и создания графиков, чтобы все работало слаженно, и компания успешно справлялась с удовлетворением спроса и ожиданий клиентов [1].

Система MRP позволяет определить сколько и в какие сроки необходимо произвести конечной продукции. Затем система определяет необходимые количества материалов и комплектующих для производства в определённый промежуток времени.

Система MRP обеспечивает неусыпный контроль за запасами. Сначала вносится вся информация, которая есть в книге учета, заказы, которые ждут отгрузки и планируются. Учитывается спецификация состава каждого изделия. Потом алгоритмы программ их используют. В результате после обработки руководитель может получить пакет из сформированных планов, предложенных корректировок и отчетов по исполнению.

Программное обеспечение (далее ПО) способно определить стратегию, с которой используются материалы на предприятии и предложить будущие закупки. В дальнейшем полученную отчетность тоже можно задействовать для составления уточненных целей.

Также появляется возможность определить «узкие места» в функционирующей компании, укажет, как уменьшить внутрипроизводственные расходы и предложит оптимальные графики производства.

К недостаткам системы MRP можно отнести:

– очень большой объём вычислений и предварительной обработки данных;

– при стремлении фирмы ещё больше уменьшить запасы или перейти на работу с малыми заказами с высокой частотой их выполнения увеличиваются логистические затраты на обработку заказов и транспортировку;

– нет чувствительности к кратковременным изменениям спроса;

– большое количество отказов из-за большой размерности системы и её сложности.

Идея MRP систем состоит в том, что любая учетная единица материалов или комплектующих, необходимых для производства изделия, должна быть в наличии в нужном промежутке времени и в нужном количестве.

Преимуществом MRP систем является формирование последовательности производственных операций с материалами и комплектующими, обеспечивающей своевременное изготовление узлов (полуфабрикатов) для реализации основного производственного плана по изготовлению готовой продукции [2].

В результате исследования ИТ класса MRP для управления автоматизации управления процессами был сформирован список наиболее «популярных» ИТ заданного класса.

Рассматривались MRP – системы, распространенные как на российском рынке, так и на зарубежном. При составлении перечня учитывалась информация российской прессы, печатные материалы фирм–разработчиков и отзывы пользователей. Также критериями выбора именно этих программ из общего числа программного обеспечения MRP – системы стали: популярность, отзывы, массовость на рынке, полнота информации о ПО.

Сравнительный анализ был выполнен применительно к судостроительным, судоремонтным предприятиям и проектно-конструкторским бюро с целью решения следующих основных задач:

Оперативно реагировать на изменения, основываясь на точной информации о состоянии дел

Моделировать и контролировать процессы в режиме реального времени

Улучшить принятие решений с анализом альтернатив и последствий

Обеспечить полное сотрудничество между подразделениями компании для использования экспертных знаний [3].

В ходе ранжирования конкурентными вариантами ИТ класса MRP (ТОП – 5) следует считать:

1. «SAP S/4HANA».
2. «SkuBrain».
3. «Oracle Demantra».
4. «Oracle NetSuite».
5. «Anaplan».

СПИСОК ЛИТЕРАТУРЫ

1. Что такое MRP (планирование потребности в материалах)? [Электронный ресурс]. URL: https://clck.ru/34MfPC (дата обращения 27.05.2023).
2. Гаврилов Д. А. Управление производством на базе стандарта MRP. 2-е изд. СПб., 2005. 416 с.
3. Алексеев А. В. Информационные технологии в жизненном цикле морской техники: курс лекций. СПб. : СПбГМТУ, 2023.

УДК 629.12, 65.011

КВАЛИМЕТРИЧЕСКОЕ РАНЖИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА «WMS» В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ И ИХ ПРАКТИЧЕСКОЕ ОСВОЕНИЕ

Головизнина Ольга Игоревна, Родоманова Кристина Сергеевна,
Бондаренко Андрей Игоревич, Алексеев Анатолий Владимирович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 194064, Россия
e-mails: golovizninaolga92@yandex.ru, kristina.rodomanova@mail.ru, bear555.ru@gmail.com, 25st1@bk.ru

Аннотация. В докладе рассматриваются технологии управления складом в защищенном исполнении и соответствующие WMS–системы на примере обеспечения жизненного цикла объектов морской техники, включая технологии квалиметрического вариантного ранжирования WMS – систем с учетом критериев и показателей обеспечения информационной защищенности и практического освоения.

Ключевые слова: технология WMS; защищенное исполнение; жизненный цикл; ранжирование; показатели защищенности.

QUALIMETRIC RANKING OF INFORMATION TECHNOLOGIES OF THE «WMS» CLASS IN ROTECTED EXECUTION AND THEIR PRACTICAL DEVELOPMENT

Goloviznina Olga, Rodomanova Kristina, Bondarenko Andrey, Alekseev Anatoly
St. Petersburg State Marine Technical University,
3 Lotsmanskaya St, St. Petersburg, 194064, Russia
e-mails: golovizninaolga92@yandex.ru, kristina.rodomanova@mail.ru, bear555.ru@gmail.com, 25st1@bk.ru

Abstract. The report examines secure warehouse management technologies and corresponding WMS systems using the example of ensuring the life cycle of marine equipment, including technologies for qualimetric variant ranking of WMS systems, taking into account the criteria and indicators for ensuring information security and practical development.

Keywords: WMS technology; protected execution; lifecycle; ranking; security indicators.

Развитие глобальных транспортных систем становится приоритетным направлением деятельности в бизнесе и политике ведущих стран мира. В России к числу таких систем относится и водный транспорт, развитие которого определяет судостроение в качестве базовой отрасли при внедрении в нее наукоемких инновационных технологий и современной организации производства. Для успешной реализации этих задач создана Объединенная судостроительная корпорация, объединившая ведущие судостроительные предприятия и проектные организации как центрального, так и регионального подчинения.

Развитие судостроения и его конкурентоспособность связаны с целым рядом факторов, снижающих себестоимость продукции. К их числу необходимо отнести такие, как сокращение затрат на проектирование и постройку судов, углубленную специализацию предприятий, уменьшение доли затрат рабочей силы за счет повышения производительности труда при одновременном обеспечении требуемого качества изделий, включая эффективное управление складами (WMS) и логистикой в целом.

Снижение затрат, связанных с проектированием и постройкой судов, невозможно сегодня без комплексного использования современных информационных технологий, в том числе в информационно защищенном исполнении (ИЗИ) в связи с наличием целого ряда угроз информационной безопасности, к числу которых в полной мере относятся WMS-технологии и соответствующие системы [1].

Еще более значимыми вопросы ИЗИ следует считать для технологий и автоматизированных систем управления предприятием (АСУП), которые включают несколько классов программных систем, которые предназначены для решения задач планирования и управления различными видами деятельности предприятия [2]. Каждый из классов АСУП имеет устоявшуюся аббревиатуру:

– управление цепочками поставок (SCM);
– планирование ресурсов предприятия (ERP);
– планирование производства (MRP, MRP II).

Одной из комплекса таких технологий является технология и реализующие ее системы управления складом WMS (Warehouse Management System), как мощный программный инструментарий, предназначенный для автоматизации управления комплексом процессов управления складом. WMS позволяет пользователю централизованно, под контролем программы с применением мобильных и голосовых терминалов, выполнять операции. Работа с внедренной системой WMS осуществляется быстро, безошибочно и эффективно, позволяя свести к минимуму потери при выполнении складских операций. Трудоемкие операции, такие как отбор и комплектация, намного быстрее и эффективнее выполнять в «настроенной» под специфику процессов WMS-системе.

Современные программы обладают развитым инструментарием, способным отслеживать поступление продукции с учетом необходимых характеристик, размещение по определенным алгоритмам, организовывать сбор и отгрузку группы заказов одновременно. Система управления складом консолидирует и хранит все произведенные транзакции. При этом данные доступны для пользователей, в online-режиме отражается вся информация о полученной, имеющейся и отгруженной продукции. В итоге WMS-система экономит много трудозатрат и времени. Помогает сократить издержки, а при эффективном использовании все расходы окупаются достаточно быстро [3]. При этом, основными автоматизируемыми процессами, в том числе минимизирующими возможные ошибки операторов (ИЗИ), как правило, являются [4]:

1. Ведение погрузо-разгрузочных работ, в том числе с использованием идентификационных этикеток.
2. Организация оптимального размещения, хранения товара и операций по его внутреннему перемещению.
3. Набор и электронная регистрация с распечаткой первичных и отчетных складских документов.
4. Организация технических способов взаимодействия персонала в процессе работы.
5. Формирование складских зон, идентификация мест хранения, адресный учет товаров в ячейках.
6. Планирование предстоящих складских операций.
7. Маршрутизация движения персонала и техники при выполнении заданий.
8. Управление резервированием номенклатурных позиций и мест хранения.
9. Автоматическое формирование алгоритма действий для персонала на основе имеющихся заданий, инструментальный контроль их исполнения.
10. Управление тарой и упаковочными материалами.
11. Планирование схемы размещения товаров при загрузке контейнеров.
12. Администрирование склада, использование данных WMS-системы в статистических, бухгалтерских, кадровых и прочих сферах управления предприятием.
13. Управление логикой размещения товаров, инвентаризацией, автоматическое выявление ошибок в действиях операторов и кладовщиков.

В этом контексте одной из сложнейших системных задач является оценка качества вариантов WMS-систем и обоснование выбора наиболее предпочтительных из них, в том числе с учетом отличия ERP-систем (на основе

технологии управления базой данных) от возможностей специализированных WMS-систем управления технологическими процессами [5].

В результате исследования информационных технологий класса WMS в ИЗИ применительно к управлению процессами склада морской стационарной платформы «Северный полюс» была сформирована система критериев и альтернативных вариантов WMS-систем в ИЗИ и решена задача обоснования оптимального выбора.

В результате квалиметрического ранжирования конкурентная способность вариантов WMS-систем в ИЗИ распределилась следующим образом (ТОП – 5):

1. Вариант WMS № 6 – «1С: Управление складом»;
2. Вариант WMS № 7 – «EME.WMS»;
3. Вариант WMS № 5 – «WMS Logistics Vision Suite»;
4. Вариант WMS № 3 – «Yarus WMS»;
5. Вариант WMS № 4 – «Gestori pro».

Полученные результаты и соответствующая база данных и знаний предназначена для системной оптимизации построения и оптимизации характеристик корпоративных систем автоматизации предприятий и организаций с учетом специфики, и соответствующих критериев WMS-систем в ИЗИ.

Пренебрежение подобными данными может привести к ошибкам системного выбора и соответствующим информационным рискам второго порядка, цена которых существенно выше.

СПИСОК ЛИТЕРАТУРЫ

1. Информационные технологии в судостроении: существующие системы, сферы и возможности их использования [Электронный ресурс] URL: https://uchimsya.com/a/qC363Pr9 (дата обращения 24.05.2023).
2. Алексеев А. В. Информационные технологии в жизненном цикле морской техники: курс лекций. СПб.: СПбГМТУ, 2023.
3. Основное назначение и применение WMS системы [Электронный ресурс] URL: https://www.toplogwms.ru/blog/sovershennaya-avtomatizatsiya-sklada-ispolzovanie-wms-sistem/ (дата обращения 24.05.2023).
4. Система WMS: как пользоваться программой управления складом [Электронный ресурс] URL: https://best-WMS.ru/WMS-system-chto-eto-kak-rabotaet/ (дата обращения 24.05.2023).
5. ERP и WMS выбор продукта для информационного управления складом [Электронный ресурс] URL: https://www.miit.ru/content (дата обращения 24.05.2023).

УДК 004.056

ЦИФРОВОЙ ДВОЙНИК ПРОГРАММНЫХ СРЕДСТВ РЕАЛИЗАЦИИ СЕРВИСА CRM В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

Егоров Ахмед Сахибович, Дуркин Илья Константинович,
Никоноров Владислав Юрьевич, Едошин Александр Дмитриевич
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 190121, Россия
e-mails: elizabeth_dewitt-bioshock@mail.ru, durkinilya@mail.ru,
albina-list@yandex.ru, alex.edoshin@yandex.ru

Аннотация. Рассмотрена технология разработки цифрового двойника (ЦД) программных средств, реализующих сервис CRM по автоматизации управления взаимоотношениями с заказчиками и клиентами в информационно защищенном исполнении. Представлен аналитический обзор бурно развивающихся технологий ЦД, основные направления и проблемы решения типовых задач, уникальная методика разработки ЦД в составе подсистем цифрового паспорта, цифровой модели, цифровой тени, управления базой данных и знаний, а также поддержки решений и информационно защищенного управления. Применительно к задачам сервиса CRM адаптирован роботизированный проектный комплекс «КСПР-23» и показана возможность использования разработанного ЦД при проектировании, эксплуатации, учебно-тренажерном обеспечении подготовки и переподготовки специалистов, включая практическую отработку задач информационной безопасности и информационного противодействия по технологии ЦД.

Ключевые слова: цифровой двойник; информационная технология CRM; безопасность данных; РПК «КСПР-23»; цифровой паспорт; цифровая тень.

DIGITAL TWIN OF SOFTWARE IMPLEMENTATION TOOLS CRM SERVICE IN PROTECTED EXECUTION

Egorov Ahmed, Durkin Ilya, Nikonorov Vladislav, Edoshin Alexander
Saint Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 190121, Russia
e-mail: elizabeth_dewitt-bioshock@mail.ru, durkinilya@mail.ru, albina-list@yandex.ru, alex.edoshin@yandex.ru

Abstract. The technology of developing a digital twin (CD) of software tools that implement a CRM service for automating the management of relationships with customers and clients in an information-protected execution is considered. An analytical review of rapidly developing data center technologies, the main directions and problems of solving typical tasks, a unique methodology for developing a data center as part of subsystems of a digital passport, digital model, digital shadow, database management and knowledge, as well as decision support and information-protected

management is presented. In relation to the tasks of the CRM service, the robotic design complex «KSPR-23» has been adapted and the possibility of using the developed data center in the design, operation, training and training support for training and retraining of specialists, including practical testing of information security and information counteraction tasks using data center technology, has been shown.

Keywords: digital double; CRM information technology; data security; RPK «KSPR-23»; digital passport; digital shadow.

В настоящее время цифровой трансформации экономики и общества различные военные структуры, компании и организации все чаще переходят на использование автоматизированных комплексов управления своими бизнес-процессами со специализированной структуризацией управления взаимодействием с заказчиками и клиентами, используя информационные технологии класса CRM (Customer Relationship Management). Достигаемая при этом цель — эффективное управление контактами, повышение удовлетворённости и лояльности заказчиков и клиентов [1].

Одной из значительных уязвимостей широкомасштабного внедрения технологий и сервисов CRM — возможность несанкционированного доступа, нарушения целостности, нелегитимного использования коммерческой и технологической информации, целенаправленные кибервторжения конкурентов и т. п. [2].

В этой связи задача защиты информации становится весьма актуальной задачей с учетом высокой динамики развития, расширения спектра и сложности используемых информационных атак и реализующих их средств, а используемые «стандартные» методы и средства защиты далеко не всегда обеспечивают безопасность данных, не смотря на значительные инвестируемые в информационную безопасность средства.

В условиях всё большего осознания важности защиты данных и гарантированного обеспечения безопасности использования информационных технологий (ИТ), а в классе CRM — в первую очередь, разработка и внедрение новой и перспективной технологии ЦД становятся всё более важным «стратегическим» шагом на пути обнаружения и предотвращения угроз безопасности, а также — для мониторинга и анализа действий пользователей, анализа и управления сложными системными процессами.

По существу ЦД представляет собой цифровую (виртуальную) интерактивную модельную «копию/близнеца» физического объекта или процесса, синхронизированную в автоматическом (роботизированном) режиме и обеспечивающую оптимизацию управленческих решений и эффективность функционирования объекта с прогнозированием (предсказанием) результатов производства качественных и конкурентно способных продуктов и услуг, с выявлением, анализом, синтезом и управлением реализации эффективных путей решения сопутствующих проблем управления и прогрессивного развития. Это позволяет отслеживать и регистрировать все операции и события, анализировать действия пользователей и системных процессов, обнаруживать аномалии и предотвращать нарушения безопасности данных [3].

Так как тема создания и использования ЦД достаточно важная, различные исследователи и разработчики в области разработки ЦД класса CRM проводят активные исследования по разработке новых методик, подходов и технологий. Существуют несколько успешных практических реализаций ЦД различных CRM [1, 2], одна из которых [3] и была детально исследована в данной работе. Однако, необходимо и дальше совершенствовать данные технологии, включая разработку новых алгоритмов обнаружения аномалий, повышение производительности и масштабируемости систем, адаптации к различным типам CRM-платформ и интеграцию с другими средствами безопасности [2].

В качестве рассматриваемой практической реализации разработки ЦД для программных средств (ПС), реализующих сервисы CRM в защищённом исполнении (ЗИ), был использован роботизированный проектный комплекс (РПК) оценки и обеспечения конкурентной способности и перспективности развития версии 2023 года (РПК «КСПР-23»), разработанный на Кафедре судовой автоматики и измерений СПбГМТУ. Данный комплекс может быть адаптирован практически к широкому спектру задач и к любому объекту информатизации, включая обеспечение комплексной безопасности, за счёт [3]:

1. Достаточно гибкой и масштабируемой архитектуры, содержащей в себе мониторинг в режиме реального времени, позволяющий своевременно выявить проблемы в работе ИТ, оптимизировать производительность, безопасность и надёжность.
2. Возможности принимать эффективные и оптимальные управленческие решения, а также обосновывать их пути реализации.
3. Системной обоснованности и целостности решения задачи эффективного использования ИТ за счёт формирования и анализа цифровых паспортов ИТ и своевременного принятия корректирующих решений за счёт использования данных мониторинга, прогнозирования и контроля.

Методика разработки ЦД для ИТ и ПС класса CRM в ЗИ заключается в назначении системы «датчиков» (имитаторов), которые имитируют определённые условия или процессы. В модуле управления базой данных и знаний РПК «КСПР-23», входящем в «3.СУБД3.1», при адаптации РПК формируется перечень имитаторов, моделирующих контроль ряда параметров. В качестве контролируемых параметров может выступать, например, параметр обеспечения безопасности данных, соблюдения регламентов доступа, целостности данных, их доступности и т.д.

Далее в модуле «2.СМПК», представляющим из себя рабочие окна, в первом из них заносятся процентные показатели имитаторов, каждый из которых соотнесён к системам ИТ, которые, в свою очередь, агрегированы в главный показатель качества — агрегированный (АПК).

Во втором окне наглядно представлено текущее состояние объекта по всем имитаторам (безопасная эксплуатация, предупреждение об возникновении аварийной ситуации, аварийная ситуация, борьба за живучесть), свойствам системы и АПК, а также прогнозируемое состояние ИТ и варианты принятия решений для предотвращения аварийной ситуации на каждый момент времени для каждой системы.

Также с использованием соответствующих макросов реализуется возможность мониторинга состояния контролируемого ПС в каждый интервал времени (мониторинга), в результате чего существует возможность наблюдать в целом состояние средств, реализующего сервис CRM, в любой момент времени и с заданным шагом мониторинга.

В результате работы с ЦД достаточно наглядно «вырисовывается» общая картина обстановки по состоянию программного средства реализации сервисов CRM на любом временном промежутке, что позволяет своевременно идентифицировать причину возникновения ошибок в работе ПС и предотвращать последующее ухудшение её функциональности и прочих свойств ЦД.

В данной работе описана лишь малая часть функциональных возможностей РПК «КСПР-23».

В данной работе была представлена разработка ЦД для ИТ класса CRM с акцентом на обеспечение высокого уровня безопасности данных. Анализируя существующие проблемы безопасности данных в ИТ класса CRM и результаты работы, можно сделать вывод, что разработанный ЦД, представленный РПК КСПР-23, обеспечивает безопасность данных в ИТ класса CRM в ЗИ.

Таким образом, разработка ЦД для ИТ и ПС класса CRM в ЗИ имеет концептуальное значение для предотвращения и обнаружения угроз безопасности, мониторинга и анализа действий пользователей и системных процессов. Существующие успешные практические реализации ЦД подтверждают значимость этого подхода, однако, необходимо продолжать совершенствовать данные технологии, включая разработку новых алгоритмов обнаружения аномалий, повышение производительности и масштабируемости систем, адаптацию к различным типам CRM-платформ и интеграцию с другими средствами безопасности.

Методика разработки ЦД для ИТ и ПС класса CRM в ЗИ основана на использовании имитаторов и моделировании определённых условий или процессов. Разработанный модуль РПК «КСПР-23» предоставляет гибкую и масштабируемую архитектуру, обеспечивающую мониторинг в режиме реального времени, принятие эффективных управленческих решений и системную обоснованность и целостность решения задачи эффективного использования ИТ.

В результате работы с разработанным ЦД в РПК «КСПР-23» показано, что достигается наглядное представление обстановки состояния ИТ класса CRM на любом временном промежутке, что позволяет идентифицировать причины возникновения ошибок в работе ИТ и предотвращать их ухудшение.

Таким образом, результаты данной работы свидетельствуют о том, что разработанный ЦД ИТ и ПС реализации сервисов CRM в ЗИ на базе РПК «КСПР-23» обеспечивает контролируемую безопасность данных, оперативную реакцию на нарушения безопасности, предотвращение утечки информации и обнаружение внутренних и внешних угроз. Реализованный подход имеет важное значение и перспективность для обеспечения безопасности информационных систем, в том числе в классе сервисов CRM и создания эффективной системы управления взаимоотношениями с заказчиками и клиентами.

СПИСОК ЛИТЕРАТУРЫ

1. Creatio [Электронный ресурс]. URL: https://www.creatio.com/crm (дата обращения: 04.05.2023).
2. Цифровой двойник. Анализ, тренды, мировой опыт. Издание первое, исправленное и дополненное. М.: АльянсПринт, 2020. 401 с.
3. Алексеев А. В. Лекционный материал по дисциплине «Информационные технологии в жизненном цикле морской техники». СПбГМТУ, 2021.
4. Речкалов А. В., Артюхов А. В., Куликов Г. Г., Новиков В. Н. [Электронный ресурс]. Концепция системного представления предметной области при формировании цифрового двойника производственного процесса машиностроительного предприятия // Вестник Уфимского государственного авиационного технического университета. 2022. № 1. С. 120-135. Текст: электронный // Лань : электронно-библиотечная система. URL: https://e.lanbook.com/journal/issue/325868 (дата обращения: 28.07.2023). Режим доступа: для авториз. пользователей.

УДК 681.3.06

КВАЛИМЕТРИЧЕСКОЕ РАНЖИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА «PDM» В ЖЦ ОМИ ТИПА АО ЦМКБ «АЛМАЗ» И ИХ ПРАКТИЧЕСКОЕ ОСВОЕНИЕ

Парастаева Елена Игоревна, Калинина Алена Михайловна,
Тюрина Наталья Анатольевна, Алексеев Анатолий Владимирович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, Санкт-Петербург, 194064, Россия
e-mails: prlena5505@mail.ru, akalinina883@gmai.com, nata9475@gmail.com, 25st1@bk.ru

Аннотация. В статье рассматриваются PDM — системы, наиболее подходящие для жизненного цикла объекта морской инфраструктуры на примере акционерного общества ЦМКБ «Алмаз». Квалиметрическое ранжирование лучших PDM – систем и их практическое освоение.

Ключевые слова: PDM; АО ЦМКБ «Алмаз»; информационные технологии; жизненный цикл; ранжирование.

QUALIMETRIC RANKING OF INFORMATION TECHNOLOGIES OF THE CLASS «PDM» IN THE HOUSING AND COMMUNAL SERVICES OF THE TYPE OF JSC CMKB «ALMAZ» AND THEIR PRACTICAL DEVELOPMENT

Parastaeva Elena, Kalinina Elena, Tyurina Natalia, Alekseev Anatoly
St. Petersburg State Marine Technical University,
3 Lotsmanskaya St, St. Petersburg, 194064, Russia
e-mails: prlena5505@mail.ru, akalinina883@gmai.com, nata9475@gmail.com, 25st1@bk.ru

Abstract. The article discusses PDM systems that are most suitable for the life cycle of a marine infrastructure facility on the example of the joint–stock company CMKB Almaz. Qualimetric ranking of the best PDM systems and their practical development.

Keywords: PDM; Almaz Central Design Bureau JSC; information technologies; life cycle; ranking.

Для судоремонтных предприятий большую роль играют наработанные базы знаний, содержащие стандартные фрагменты различных графиков проектов ремонта, допускающие в сжатые сроки оценить реальную продолжительность и стоимость выполнения будущего судоремонта.

Решение всех этих, а также многих других задач управления проектами позволяет обеспечить и упростить специализированная информационная система управления проектами (ИСУП). Наличие данной системы на судостроительных и судоремонтных заводах является насущной необходимостью.

На судостроительных предприятиях применяется множество различных информационных систем, многие из которых могут быть интегрированы с ИСУП. В частности, к ним можно отнести CAD/CAM-системы, системы документооборота, электронные архивы, PDM/PLM-системы и т. д [1].

PDM-система (англ. Product Data Management — система управления данными об изделии) — организационно-техническая система, обеспечивающая управление всей информацией об изделии. При этом в качестве изделий могут рассматриваться различные сложные технические объекты (корабли и автомобили, самолеты и ракеты, компьютерные сети и др.) [2].

Роль PDM-технологии состоит в том, чтобы сделать информационные процессы максимально прозрачными и управляемыми. Основным методом, применяемым для этого, является повышение доступности данных для всех участников ЖЦ изделия, то требует интеграции данных об изделии в логически единую информационную модель.

Пользователями PDM-системы выступают все сотрудники предприятий-участников ЖЦ изделия (конструкторы, технологи, работники технического архива), а также служащие, работающие в других предметных областях: сбыт, маркетинг, снабжение, финансы, сервис, эксплуатация и т. п. PDM-система обеспечивает все потребности пользователя, начиная от просмотра спецификации узла и кончая изменением твердотельной модели детали или утверждением измененной детали начальником. При необходимости PDM-система пользуется помощью других систем для обработки данных (например, САПР), самостоятельно определяя, какое именно внешнее приложение необходимо запустить для обработки той или иной информации [1].

Перечень функций PDM-системы:

1. Управление хранением данных и документов. Все данные и документы в PDM-системе хранятся в специальной подсистеме (хранилище данных), которая обеспечивает их целостность, организует доступ к ним в соответствии с правами доступа и позволяет осуществлять их поиск. Данные документы являются электронными, т.е. обладают электронной подписью.

2. Управление процессами. PDM-система отслеживает все операции пользователей с данными, в том числе следит за версиями. Кроме того, PDM-система управляет потоком работ (например, в процессе проектирования изделия) и занимается протоколированием действий пользователей и изменений данных.

3. Управление составом изделия. PDM-система содержит информацию о составе изделия, его вариантах. Важной особенностью является наличие нескольких представлений состава изделия для различных предметных областей (конструкторский состав, технологический состав, маркетинговый состав и т.д.).

4. Классификация. PDM-система позволяет производить распределение изделий и документов в соответствии с различными классификаторами. Это может быть использовано при поиске продукта с нужными характеристиками с целью его повторного использования или для автоматизации присваивания обозначений компонентам изделия.

Использование PDM-системы ведет к уменьшению времени проектирования на 20-30 %. Сокращение сроков выхода изделия на рынок связан в первую очередь с повышением эффективности процесса проектирования, вызванного применением PDM-системы. Оно имеет четыре аспекта:

1. PDM-система избавляет конструктора от непроизводительных затрат времени, связанных с исключительно с поиском, копированием и архивированием данных, что при работе с бумажными носителями составляет 25…30 % его времени.

2. PDM-система позволяет улучшить коммуникации между конструкторами, технологами и другими участниками ЖЦ изделия за счет применения технологий параллельного проектирования и значительно расширяет количество изменений, перенося большую их часть на этап проектирования (более раннее выявление ошибок).

3. Благодаря упорядочиванию потока работ значительно сокращается стоимость изменения (в первую очередь, из-за исключения временных потерь).

4. PDM-система практически избавляет конструктора от синдрома «изобретения велосипеда», делает реально возможным широкое заимствование и повторное использование уже спроектированных деталей. Ранее было проще заново спроектировать узел, чем искать уже существующий, перелопачивая горы документации. Таким образом, PDM-система доводит количество заимствованных компонентов в изделии до 80 % [1].

В результате анализа ИТ класса PDM для проектирования и производства ОМИ типа АО «ЦМКБ «Алмаз» следует считать конкурентными вариантами PDM-системы следующие программы:

1) «Teamcenter (PDM/PLM)»;
2) «ЛОЦМАН:PLM»;
3) «PDM STEP Suite»;
4) «BaanPDM»;
5) «ENOVIA»;
6) «Windchill».

Однако приведенные оценки следует рассматривать в качестве предварительных, требующих уточнения с учетом угроз развития таких как: технологическая зависимость, возможность появления санкций, использование систем, которых нет в интеграции.

Точность квалимерического сравнения ИТ класса PDM была обеспечена использованием данных, предоставленных на официальных сайтах выбранных PDM-систем, а также выбором критериев, отражающих различные аспекты их реализации на производстве [3].

В ходе проведенного сравнительного анализа, следует считать оптимальным вариантом по всем моделям — «Teamcenter(PDM/PLM)».

«Teamcenter (PDM/PLM)» — это система, обеспечивающая организацию коллективной работы сотрудников предприятия (группы предприятий) с данными об изделии и связанных с ним процессах на всех этапах его жизненного цикла. Teamcenter — это единая платформа, состоящая из набора взаимосвязанных компонентов, обеспечивающих непрерывную поддержку и управление всем жизненным циклом изделия и процессов предприятия.

Teamcenter служит не только единым источником знаний об изделии, но предоставляет широкий набор механизмов доступа к этим данным и управления бизнес процессами на всех этапах жизненного цикла. Кроме того, система обеспечивает одновременную работу на территориально удаленных площадках в т.ч. удаленный доступ и/или пакетные режимы обмена данными, а также гибкую систему интеграции и обмена данными с ERP системой (и системами других классов) предприятия [4].

СПИСОК ЛИТЕРАТУРЫ

1. Система управления данными об изделии — PDM [Электронный ресурс]. URL: https://studfile.net/preview/2652078/page:11/ (дата обращения 14.03.2023).
2. Алексеев А. В. Информационные технологии в жизненном цикле морской техники: курс лекций. СПб.: СПбГМТУ, 2023.
3. Кваскov Е. В. Квалиметрическое ранжирование информационных технологий класса PDM в жизненном цикле объекта морской техники типа «НИС Гидрологическое» и их практическое освоение. СПбГМТУ, 2021;
4. Teamcenter (PDM\PLM) [электронный ресурс]. URL: https://nslabs.ru/programmnoe-obespechenie/resheniya-siemens-plm-software/teamcenter-pdm-plm/ (дата обращения 2023-04-08).

УДК 519.687.1

ЗАДАЧА ПОИСКА ОПТИМАЛЬНОГО ПОЛОЖЕНИЯ ЦЕНТРА УПРАВЛЕНИЯ В БЕЗОПАСНОМ ИСПОЛНЕНИИ В ВЫСОТНОМ ЗДАНИИ МОРСКОЙ ИНФРАСТРУКТУРЫ

Плотников Павел Владимирович[1], Алексеев Сергей Алексеевич[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп.1, лит. А, Ж, Санкт-Петербург, 193232, Россия

[2] Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

e-mails: ksgati@yandex.ru, pavplot@gmail.com

Аннотация. В статье рассматривается задача, суть которой состоит в минимизации функции оценки расстояния до самой дальней камеры, чтобы снизить влияние шумов и повысить качество сигнала, благодаря уменьшению длины кабеля, а также увеличения зоны охвата видеонаблюдения при минимальных расходах на материалы. Приведен алгоритм расчета оптимального местоположения центра управления в безопасном исполнении на плоскости и в 3D-пространстве в реальном времени. Процесс поиска решения может быть автоматическим, проведен вычислительными устройствами в реальном времени, при этом полученные решения являются численными и точными.

Ключевые слова: задача размещения Ролса; задача оптимизации; тропическая оптимизация; прямоугольная метрика; идемпотентное полуполе; полное решение.

THE TASK OF FINDING THE OPTIMAL POSITION OF THE CONTROL CENTER IN A SAFE EXECUTION IN A HIGH-RISE BUILDING OF THE MARINE INFRASTRUCTURE

Plotnikov Pavel[1], Alekseev Sergey[2]
[1]St. Petersburg State University of Telecommunications named after Prof. M. A. Bonch-Bruevich
22 Bolshevikov Av, Bld 1, lit. A, Zh, St. Petersburg, 193232, Russia
[2]Admiral S.O. Makarov Federal University of Marine and River Fleet
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: pavplot@gmail.com, ksgati@yandex.ru

Abstract. The article considers the task, the essence of which is to minimize the function of estimating the distance to the furthest camera in order to reduce the influence of noise and improve signal quality by reducing the length of the cable, as well as increasing the coverage area of video surveillance with minimal material costs. An algorithm for calculating the optimal location of the control center in a safe execution on a plane and in 3D space in real time is given. The process of finding a solution can be automatic, carried out by computing devices in real time, while the solutions obtained are numerical and accurate.

Keywords: Rolls placement problem; optimization problem; tropical optimization; rectangular metric; idempotent half-field; complete solution.

Одной из перспективных и быстро развивающихся областей прикладной математики и алгебраической информатики является тропическая математика, которая связана с изучением теории и приложений полуколец с идемпотентным сложением. В технике, экономике и управлении при автоматизации и информатизации различных процессов достаточно часто можно встретить оптимизационные задачи, которые могут быть сформулированы и решены в терминах тропической математики (задачи тропической оптимизации).

Существует важный с практической точки зрения класс задач оптимизации, возникающих при оптимальном проектировании информационных систем и процессов (оптимизация структуры информационной системы, оптимизация топологии сети передачи данных, оптимизация архитектуры распределенных систем обработки данных и др.), в которых требуется найти наилучший способ разместить объект без ограничений или с дополнительными ограничениями на допустимую область размещения. Такую задачу часто называют задачей 1-центра, которая представляет важный класс задач оптимизации и находит широкое применение. Задачу в самом общем случае можно сформулировать так: задано множество объектов информационной системы, в которых может осуществляться создание, обработка или потребление информации, допустимая область размещения целевого объекта и функция для расчета характеристик взаимосвязи целевого объекта и заданных объектов, являющихся элементами рассматриваемой системы (целевая функция). Необходимо найти оптимальное положение объекта с целью оптимизации значения характеристики, описывающей его взаимосвязи с заданными объектами.

Основная часть. Решение задачи находит свое применение на практике в различных областях, связанных с проектированием процессов создания, накопления и обработки информации, исследованием принципов создания и функционирования аппаратных средств автоматизации, моделированием информационных потребностей коллективных и индивидуальных пользователей и способов их удовлетворения, разработкой и анализом моделей информационных процессов и структур и др.

Существенную роль при решении таких задач играет выбор метрики, при помощи которой осуществляется вычисление значения целевой функции. В случае евклидовой метрики, задача, известная также как задача о наименьшей ограничивающей сфере, имеет геометрическое решение и итерационное решение в виде алгоритма. Большим прикладным значением обладает решение минимаксной задачи размещения с прямоугольной метрикой. Такого рода оптимизационную задачу называют задачей Ролса или задачей посыльного. Известно геометрическое решение этой задачи, а также решение с помощью методов ли¬нейного программирования, в частности, с использованием симплекс-метода.

На практике рассматриваемый класс задач может встречаться, например, при проектировании размещения центров управления, хранения и обработки данных, собранных с видеокамер системы видеонаблюдения в высотном здании морской инфраструктуры [1-3].

Решение задач пространственного (3D) размещения объектов зависят от метрики, в которой вычисляется расстояние между объектами. В данной статье рассматривается решение задач пространственного размещения объектов в прямоугольной метрике с использованием методов тропической (идемпотентной) математики.

В статье рассматривается минимаксная задача (Ролса) размещения на плоскости и в 3D пространстве с прямоугольной метрикой, которая может быть представлена в терминах идемпотентной алгебры. Подход к решению основывается на преобразовании задач размещения к экстремальным задачам. В ходе исследования были получены аналитические зависимости, предлагающие на основе известных данных о размещении обслуживаемых объектов (видеокамер) найти оптимальные зоны размещения обслуживающих их объектов (маршрутизаторов, серверов, и др.). При этом требуется разместить новый обслуживающий объект так, чтобы минимизировать расстояние от этого объекта до самого удаленного из обслуживаемых объектов.

Полученные результаты позволяют сделать вывод, что решением задачи может быть не только одна точка, где размещение будет оптимальным, а зона или поле оптимального размещения. Это весьма важно с прикладных позиций, т. к. позволяет учесть возможные ограничения задачи.

Важным преимуществом предлагаемого алгоритма является простота итоговых формульных зависимостей, позволяющая легко использовать его при создании и развитии информационных и иных систем искусственного интеллекта.

Решение задачи оптимального размещения центрального сервера управления сетью локальных видеокамер в высотном здании морской инфраструктуры. Общая формулировка задачи оптимизации на плоскости. Пусть необходимо собирать, обрабатывать и хранить информацию, поступающую с n видеокамер локальной сети. Координаты этих видеокамер задаются векторами vi = (v1i, v2i)T R2, где i = 1, ... , n. Задача размещения состоит в том, чтобы найти оптимальное местоположение центрального сервера (центра управления), которое задано неизвестным вектором x = (x1, x2)T. При этом, необходимо минимизировать расстояние от этого сервера до самой дальней видеокамеры. Основная задача (критерий) состоит в снижении величины затухания сигнала, которое прямо пропорционально расстоянию, например: длине кабеля, что соответственно оправдывает минимаксную постановку задачи.

Для решения задачи 1-центра существует три подхода:

1) геометрический подход с нахождением оптимального положения управляющего объекта методами построений;

2) итерационный метод моделирования решения задачи размещения с использованием компьютерных мощностей;

3) получение решения в явном виде методами идемпотентной алгебры.

Вывод: для решения описанных выше задач получены полные аналитические решения в явном виде, их использование при решении минимаксных задач размещения позволяет понизить алгоритмическую сложность вычислений, в сравнении с известными итерационными подходами. Предложенный в статье| алгоритм нахождения оптимальной области размещения видеокамер как на плоскости, так и в трехмерном пространстве с прямоугольной метрикой на основе геометрического подхода, имеет низкую алгоритмическую сложность.

В статье рассмотрена минимаксная задача размещения точечного объекта в двух и трехмерном пространстве с прямоугольной метрикой. Такая задача встречается на практике, например, при размещении центра управления системой камер видеонаблюдения в здании. Разработанный и представленный в статье алгоритм можно применить в области проектирования и создания аппаратных средств автоматизации решения задач автоматической оптимизации построения сложных информационных систем и их сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Плотников П. В. Решение минимаксных задач размещения на плоскости с прямоугольной метрикой на основе методов идемпотентной алгебры: автореферат диссертации. СПб., 2018. 18 с.
2. Плотников П. В., Н. К. Кривулин. Прямое решение минимаксной задачи размещения в прямоугольной области на плоскости с прямоугольной метрикой // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. СПб., 2018. Т. 14. № 2. С. 116-130.
3. Плотников П. В., Кривулин Н. К. Решение минимаксной задачи размещения в трехмерном пространстве с прямоугольной метрикой // Компьютерные инструменты в образовании. СПб., 2018. № 1. С. 31-50.

УДК 629.561

ПРИНЦИПЫ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ НАУЧНО-ПРОИЗВОДСТВЕННЫХ ОБЪЕДИНЕНИЙ МОРСКОЙ ИНФРАСТРУКТУРЫ

Рябков Яков Игоревич[1], Алексеев Сергей Алексеевич[2], Артемов Станислав Игоревич[3]

[1]Военно-космическая академия имени А. Ф. Можайского
Ждановская ул., 13, Санкт-Петербург,197198, Россия

[2] Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

[3]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: yakovrt@mail.ru, ksgati@yandex.ru, pushokcheck@yandex.ru

Аннотация. Появление и развитие наукоемких отраслей производства в России связано с развитием научно производственных объединений (НПО). Целью данной статьи является выявление отраслевых структурных и производственных особенностей НПО морской инфраструктуры в России, их роли в развитии потенциала страны и рассмотрение возможностей повышения эффективности функционирования. Данные исследования в совокупности позволят сформировать комплексное представление о сущности и особенностях НПО в России, что позволит в дальнейшем совершенствовать эффективную организацию и управление в защищенном исполнении предприятиями наукоемких отраслей.

Ключевые слова: организационное управление; научно-производственное объединение; автоматизация управления; социальная организационно-техническая система**.**

PRINCIPLES OF AUTOMATION OF MANAGEMENT IN THE PROTECTED EXECUTION OF SCIENTIFIC AND INDUSTRIAL ASSOCIATIONS OF MARINE INFRASTRUCTURE

Ryabkov Yakov[1], Alekseev Sergey[2], Artemov Stanislav[3]

[1]Military Space Academy named after A. F. Mozhaisky
13 Zhdanovskaya St, St. Petersburg, 197198, Russia

[2]Federal University of the Sea and River Fleet named after Admiral S.O. Makarov,
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
[3]Sankt-St. Petersburg State Electrotechnical University «LETI» named after V.I. Ulyanov (Lenin)
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: yakovrt@mail.ru, ksgati@yandex.ru, pushokcheck@yandex.ru

Abstract. The emergence and development of knowledge-intensive industries in Russia is associated with the development of scientific production associations (NGOs). The purpose of this article is to identify the sectoral structural and production features of marine infrastructure NGOs in Russia, their role in the development of the country's potential and to consider ways to improve the efficiency of functioning. These studies together will allow us to form a comprehensive understanding of the nature and features of NGOs in Russia, which will further improve the effective organization and management in the protected execution of knowledge-intensive industries.

Keywords: automation of management; organizational management; scientific and production association; social organizational and technical system.

Главным отличием НПО от производственных предприятий состоит в том, что НПО представляют собой совокупность не только средств производства, служащих и работников, но и коллектива ученых, имеющих высокий уровень образования в производственной области. Достижение высокого уровня конкурентоспособности выпускаемых изделий в НПО возможно, если при его производстве используется высокий процент интеллектуальных ресурсов, выпускается высокотехнологичная продукция. Порядок планирования деятельности НПО морской инфраструктуры сохраняет обособленность подразделений внутри НПО с одной стороны, по промышленности, с другой — по направлениям отраслей науки. К научным продуктам можно отнести знания и информацию в виде монографий, отчетов, рекомендаций, чертежей, проектов, опытных образцов, которые обладают новизной.

Все рабочие места руководства НПО, руководителей подразделений и рабочих смен оснащены средствами, использующими цифровые технологии различной конфигурации, которые функционируют при поддержке определенного программного и информационного обеспечения. В руководство НПО морской инфраструктуры в России, как правило, входят: начальник, первый заместитель начальника НПО и заместители начальника НПО по специальным направлениям. НПО состоит из отделов, специальных центров, отделений и групп.

Все изложенное выше позволяет сделать вывод о том, что НПО морской инфраструктуры является, во-первых, социальной системой, в состав которой входят как сотрудники руководства НПО, отделов, отделений и групп, так и персонал учреждений, организаций и объектов, которые совместно с сотрудниками НПО обеспечивают функции сбора оперативной информации, состоянии функциональных и территориальных подсистем и оперативной координации действий органов повседневного управления. Во-вторых, НПО совместно с учреждениями, организациями и объектами управления является организационной системой, т.е. системой иерархической с горизонтальными и вертикальными связями между ее компонентами. В-третьих, НПО, сотрудники которого сами работают на АРМ и управляют научными и производственными подразделениями, которые также оснащены рядом цифровой техникой, является технической системой, так как его персонал на всех уровнях управления использует средства вычислительной техники с соответствующим программным и информационным обеспечением.

Таким образом, НПО морской инфраструктуры можно рассматривать, как социальные организационно-технические системы (СОТС), относящиеся к классу сложных, иерархических, самоорганизующихся и самоадаптирующихся человеко-машинных систем (ЧМС), в которых персонал управленцев работает, в том числе, на АРМ. Вывод: для исследования законов функционирования НПО морской инфраструктуры можно использовать уже известные, рабочие законы, применяемые при исследовании ЧМС. Следовательно, НПО морской инфраструктуры, как СОТС представляет собой разновидность ЧМС вида «группа операторов — корпоративная сеть» (ГОКС).

Проведенный анализ структуры и функций НПО морской инфраструктуры, как СОТС показывает, что процесс управления таким сложным иерархическим объектом может осуществляться эффективно в случае, если все компоненты такой СОТС будут объединены в региональную вычислительную корпоративную сеть (КС). Такая сеть является сетью передачи данных, в узлах которой располагаются ЭВМ и персонал, их использующий. Основной задачей КС, моделирующей информационные технологии, реализуемые в рамках НПО, как СОТС, является передача информации между различными подразделениями НПО.

Под автоматизацией процессов управления в СОТС принято понимать комплекс мероприятий, направленных на внедрение средств вычислительной техники (СВТ) и современных информационных технологий (ИТ) в работу органов управления НПО, с целью создания условий повышения эффективности деятельности лица, принимающего решение (ЛПР) при выполнении производственного задания.

Оценка эффективности требует наличия критерия и показателя эффективности. Показатель эффективности — системная мера, количественно характеризующая степень выполнения системой цели функционирования, поставленной задачи и функции управления, или количественная оценка свойства, выбранного в качестве характеристики эффективности системы. Критерий эффективности — это правило или способ принятия какого-либо управленческого решения, осуществления того или иного управляющего воздействия на основе анализа выработанного показателя эффективности.

Одной из самых важных задач при оценке эффективности автоматизации управления НПО является выбор или формулировка показателя эффективности. Во-первых, этот показатель (интегральный) должен описать степень проявления автоматизированной системой своего главного, интегрального свойства, определяющего цель ее функционирования. Во-вторых, такой показатель должен складываться из ряда показателей, характеризующих частные, второстепенные свойства НПО, которые в разной степени и часто противоречиво влияют на интегральный показатель эффективности. В-третьих, интегральный показатель должен учитывать многоцелевой характер функционирования НПО. В-четвертых, реально существующая иерархичность НПО, многоуровневость целей ее функционирования могут приводить к крайнему усложнению формулировки или выбора показателя эффективности автоматизированной системы, осуществляющей управление СОТС. Практика показывает, что, как правило, получить точные значения частных и общих показателей эффективности выбранной степени автоматизации управления такой сложной системы, как НПО нереально. Это можно сделать только в том случае, если в модели процесса функционирования НПО будет корректно учтено влияние автоматизации управления на качество творческого процесса выработки управленческих решений органом управления во главе с ЛПР и их практическую реализацию. Невозможность моделирования творческих процессов делает уровень показателей, характеризующих процессы принятия решений и контроля их исполнения, не столько научно-модельным, сколько вербально-описательным, т.е. только качественным. Показатели организационно-технической эффективности автоматизации управления в совокупности должны характеризовать все стороны обеспечения средствами автоматизации эффективной работы органа управления НПО во главе с ЛПР по выработке управленческих решений.

Из сказанного выше может быть сделан вывод о том, что наиболее важным в конкретном решении задачи выбора степени автоматизации управления функционированием НПО, является уяснение непосредственных целей, задач и функций управления НПО и ее компонентами. Не менее важной задачей при выборе систем, средств и методов автоматизации управления, обеспечивающих построение математических моделей и собственно моделирование процессов функционирования НПО, является адекватное использование математического аппарата, формализующего названный процесс управления.

СПИСОК ЛИТЕРАТУРЫ

1. Рябков Я. И., Алексеев С. А., Артемов С. И. Повышение эффективности управления маломерными судами в сложной обстановке // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция Региональная информатика (РИ-2022). Материалы конференции. СПб. : СПОИСУ, 2022. 626 с.
2. Алексеев С.А. Автоматизация процессов управления социальными организационно-техническими системами // Научное обозрение. М., 2009. № 4. С. 72-77.
3. Алексеев С. А. Оценка характеристик процесса функционирования системы «оператор (группа операторов) — корпоративная сеть» МЧС // Проблемы управления рисками в техносфере. СПб, 2008. №2. С. 50-56.
4. Алексеев С. А. Концепция создания единого информационного пространства социальной организационно-технической системы // Сборник трудов. Первого СПб. конгресса Проф. образование, наука, инновации в XXI веке. СПб. : ГУП УИТМО, 2007.

УДК 004.056

ФОРМИРОВАНИЕ СПИСКА РЕКОМЕНДАЦИЙ ДЛЯ МОДЕРНИЗАЦИИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО РЕЗУЛЬТАТАМ ОЦЕНКИ УРОВНЯ ЗРЕЛОСТИ ПРЕДПРИЯТИЯ

Тарасов Валентин Сергеевич, Кудинова Екатерина Андреевна
Владивостокский государственный университет «ВВГУ»
Гоголя ул., 41, Владивосток, 690014, Россия
e-mails: katyku221133@gmail.com, Vals.tarasov@gmail.com

Аннотация. В данном докладе представлен инновационный метод оценки уровня зрелости системы обеспечения информационной безопасности на предприятии морской отрасли, взятый на примере компании АО «Восточная Верфь». Автор представляет результаты оценки, проведенной на основе созданных им метрик. По результатам оценки сформирован список рекомендаций для проведения мероприятий по модернизации системы информационной безопасности.

Ключевые слова: СОИБ; информационная безопасность; уровни зрелости; модель зрелости; модернизация СОИБ; организационно-технические мероприятия; инженерно-технические мероприятия.

FORMATION OF A LIST OF RECOMMENDATIONS FOR MODERNIZING THE INFORMATION SECURITY SYSTEM BASED ON THE RESULTS OF ASSESSING THE ENTERPRISE MATURITY LEVEL

Tarasov Valentin, Kudinova Ekaterina
Vladivostok State University «VSU»
41 Gogol St, Vladivostok, 690014, Russia
e-mails: katyku221133@gmail.com, Vals.tarasov@gmail.com

Abstract. This report presents an innovative method for assessing the level of maturity of the information security system at an enterprise in the maritime industry, taken as an example from the company JSC Vostochnaya Verf. The

author presents the results of an assessment based on the metrics he created. Based on the assessment results, a list of recommendations was compiled for carrying out measures to modernize the information security system.

Keywords: Information security system; information security; maturity levels; maturity model; modernization of information security system; organizational and technical measures; engineering measures.

На судостроительных предприятиях в условиях развития информационного общества возникает острая необходимость обеспечения высокого уровня защиты информации. В таком случае необходимо автоматизировать и модернизировать системы обеспечения информационной безопасности (СОИБ) [1, 2]. Для модернизации прежде всего необходимо провести оценку уровня зрелости предприятия. Уровень зрелости даст численную оценку уровня зрелости и поможет выявить слабые и сильные стороны предприятия в области информационной безопасности. На данный момент существуют различные подходы к оценке уровня зрелости предприятий. Сравнение таких моделей приведено в [3]. Однако, ни одна из существующих моделей не удовлетворяет в полной мере потребностям судостроительной компании АО «Восточная Верфь». В связи с этим возникла необходимость в разработке авторской системы метрик.

По результатам оценки были выделены сильные и слабые стороны предприятия с точки зрения обеспечения степени цифровой зрелости. Так, основными преимуществами предприятия являются информационно-техническая обеспеченности, соответствие требованиям регуляторов и образование сотрудников в сфере ИБ. Слабыми же сторонами являются отсутствие систем информационного управления безопасностью, отсутствие периодичного обучения сотрудников, а также внутренняя нормативная документация не является исчерпывающей с точки зрения информационной безопасности.

Таким образом, по результатам оценки были сформированы рекомендации. Осуществление модернизации необходимо проводить в два этапа:

1. Провести организационно-технические и инженерно-технические мероприятия. В том числе определить стратегию развития и модернизации СОИБ и выстроить систему защиты на всех ее уровнях.
2. Внедрить ряд специализированных систем, осуществляющих управление и мониторинг событий ИБ.

После реализации обоих этапов необходимо провести тестирование и, в случае низких показателей, повторить комплекс мероприятий начиная с оценки по разработанной метрике, оценка полученных результатов, затем проведение первого и второго этапа и повторное тестирование.

По результатам проделанной работы был предложен список мероприятий по модернизации СОИБ, а также стратегию по повышению уровня зрелости предприятия с точки зрения информационной безопасности по разработанной автором системе метрик.

СПИСОК ЛИТЕРАТУРЫ

1. Трунова А. В. Обеспечение информационной безопасности предприятия // Современные инновации. 2018. №4 (26). С. 33-35.
2. Корчак В. Ю., Ефимова Н. С., Калачанов В. В., Давыдов Д. А. Развитие средств информационной безопасности для роста конкурентоустойчивости предприятия // Компетентность. 2017. № 8 (149). С. 6–12.
3. Милославская Н., Сагиров Р. Обзор моделей зрелости процессов управления информационной безопасностью // Безопасность информационных технологий. М.: МИФИ, 2015. Т. 22. № 2. С. 76-84.

УДК 65.011

РАНЖИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА «FM» В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Юрков Антон Николаевич
Санкт-Петербургский государственный морской технический университет
Лоцманская ул. 3, Санкт-Петербург, 194064, Россия
e-mail: toxa-boks@yandex.ru

Аннотация. Практика внедрения новых информационных технологий (ИТ) предусматривает необходимость количественного ранжирования реализующих их программных комплексов (ПК) по системе критериев предпочтений, учитывающих специфику объектов внедрения, включая необходимость обеспечения заданного уровня информационной безопасности (ИБ). В докладе рассматривается технология и результаты ранжирования программных средств в классе информационных технологий финансового менеджмента, FM-системы с использованием роботизированного проектного комплекса «АСОР-22.4-ИБ» применительно к решению задач на всех стадиях жизненного цикла судовых электроэнергетических систем (ЭЭС) подводных лодок (ПЛ). В систему критериев оценки информационной безопасности FM-систем вошли значение Обобщенного уровня качества защиты контента с грифом не ниже «Конфиденциально» по данным сертификации, функционально-сервисные преимущества, а также уровень имиджа на рынке и объем продаж. Показано, что оптимальным в этом контексте следует считать выбор программного комплекса «1С:Бухгалтерия», имеющего конкурентное преимущество более 1,5 % по отношению к ПК «Инфо-Бухгалтер».

Ключевые слова: FM-системы; защищенное исполнение; информационные технологии; жизненный цикл; ранжирование; импортозамещение.

RANKING OF INFORMATION TECHNOLOGIES CLASS «FM» IN A PROTECTED VERSION

Yurkov Anton
Saint Petersburg State Marine Technical University
3 Lotsmanskaya St, St. Petersburg, 194064, Russia
e-mail: toxa-boks@yandex.ru

Abstract. The practice of introducing new information technologies (IT) provides for the need for quantitative ranking of software complexes (PCs) implementing them according to a system of preference criteria that take into account the specifics of the implementation objects, including the need to ensure a given level of information security (IS). The report examines the technology and results of ranking software tools in the class of financial management information technologies, FM systems using the ASOR-22.4-IB robotic design complex in relation to solving problems at all stages of the life cycle of marine electric power systems (EES) of submarines (submarines). The system of criteria for assessing the information security of FM systems includes the value of a Generalized level of quality of content protection with a stamp not lower than «Confidential» according to certification data, functional and service advantages, as well as the level of image on the market and sales volume. It is shown that the choice of the 1C software package should be considered optimal in this context.:Accounting», which has a competitive advantage of more than 1.5% in relation to the PC «Info-Accountant».

Keywords: FM systems; secure execution; information technology; life cycle; ranking; import substitution.

Системы управления данными об изделии используются на всех этапах проектирования, позволяя осуществлять режим коллективного проектирования, автоматизируя функции управления, связанные с этим режимом: назначение и обеспечение квалитета ответственности, разграничение прав доступа к данным, ведение и актуализация базы данных проекта и т.д. В первую очередь системы FM упрощают передачу данных между отделами предприятия и доступ к финансовой информации, необходимой для работы в разных программных системах. Использование этих систем на предприятии существенно улучшает взаимодействие подразделений, уменьшает бумажный документооборот, повышает эффективность управления экономической деятельностью.

Так, FM — система управляет в ряде задач связанными системами автоматизированного проектирования (САПР), а также автоматизированной системой управления предприятием (АСУП) [1, 2].

Наиболее типичные в этом случае этом задачи, решаемые при помощи FM-систем:

– оптимизация расходов в каждом из производственных сегментов;
– обеспечение текущей финансовой устойчивости предприятия;
– обеспечение минимизации финансового риска на предприятии;
– обеспечение наиболее эффективного использования финансовых ресурсов.

Использование ИТ класса FM приносит предприятию немалые выгоды, главные из которых:

– ускорение выпуска новой документации;
– сокращение издержек путем замены физических документов виртуальными;
– экономия за счет многократного использования типовых проектных данных;
– расширение возможностей комплексной оптимизации расходов;
– снижение затрат с помощью полной интеграции инженерного документооборота.

В результате исследования ИТ класса FM для поддержания финансовой стабильности и недопущения убытков применительно к условиям жизненного цикла ЭЭС ПЛ была актуализирована база данных и знаний (БДЗ) роботизированного проектного комплекса (РПК) «АСОР-22.4-ИБ» за период с 1.09.2022 по 15.05.2023 развития ИТ заданного класса (финансового менеджмента) с использованием данных Государственного реестра сертифицированных средств защиты информации. При этом, наиболее значимым критерием и наиболее объективным был определен критерий ОУС — Обобщенный показатель качества защиты контента с грифом не ниже «Конфиденциально» по данным сертификации.

Более того, рассматривались FM-системы, преимущественно, российского рынка. В настоящее время, когда экономика РФ находится под санкциями, задача импортозамещения является одной из обязательных.

При актуализации БДЗ учитывалась также информация российской прессы [3], печатные материалы фирм-разработчиков и отзывы пользователей.

Также критериями выбора ПК из общего числа программного обеспечения (далее ПО) FM-систем стали: известность, массовость на рынке, полнота информации о технологиях FM и реализующих ее ПК [4-6].

Данный квалиметрический сравнительный анализ был выполнен применительно к судостроительному предприятию при управлении жизненным циклом ЭЭС ПЛ с целью решения следующих основных задач:

– оптимизации финансовых затрат, включая среди аспектов экономической безопасности факторов обеспечения ИБ по ключевым критериям конфиденциальности данных, их доступности и целостности;
– снижения сроков обработки и учета порядка значимости информации;
– оценки возможности предприятия.

В результате квалиметрического сравнения (ранжирования) ПК, реализующих соответствующие информационные технологии класса «FM» применительно к условиям судостроительного предприятия при управлении жизненным циклом ЭЭС ПЛ, был определен с использованием РПК «АСОР-22.4-ИБ» рейтинговый ряд ТОР-5, в который вошли следующие ПК:

– 1С:Бухгалтерия,
– Инфо-Бухгалтер,
– Комплексная система управления предприятием «БЭСТ»,
– Автоматизация бухучета с помощью программы Парус,
– Программы автоматизации бухучета компании ИНФОСОФТ.

В ходе квалиметрического ранжирования информационных технологий класса FM применительно к решению задач жизненного цикла ЭЭС ПЛ результаты исследования подтвердили высокую эффективность применения ИТ класса FM и их реализации в ПК «1С:Бухгалтерия», определены преимущества и недостатки его эксплуатации и получены следующие основные результаты:

1. Сформулированы оптимальные направления и перспективность цифровой трансформации проектирования и отрасли судостроения в целом.

2. Конкурентно способным программным комплексом (лидером) среди ИТ класса FM следует считать ПК «1С:Бухгалтерия» при конкурентном преимуществе в сравнении с ближайшим аналогом «ИНФО-Бухгалтер» составляет порядка 1,5 %.

3. Данный результат следует считать весьма существенным, а широкомасштабное освоение и внедрение ПК «1С:Бухгалтерия» при ожидаемой успешности внедрения порядка 90% — перспективным организационно-техническим решением в обеспечение цифровой трансформации судостроительных предприятий при создании и эксплуатации ЭЭС ПЛ и отрасли судостроения в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Финансовый менеджмент [электронный ресурс]. URL:https://ru.wikipedia.org/wiki/Финансовый_менеджмент (дата обращения: 26.07.2023).
2. Алексеев А. В. Материал лекций Информационные технологии в жизненном цикле морской техники.
3. ТОП-7. Лучшие бухгалтерские программы на 2023 год для малого и среднего бизнеса [Электронный ресурс]. URL:.https://www.ib.ru/wiki/10591 (дата обращения: 26.07.2023).
4. Ергин Д. А. гр.2162 — СР по дисциплине: «Информационные технологии в жизненном цикле морской техники» тема: «Квалиметрическое ранжирование информационных технологий класса FM, а также лучших практик их освоения в ЖЦ ОМТ типа ЭЭС ледокола «Арктика» и их практическое освоение»
5. Теория практики. ИТвЖЦ МТ. УМК Теория практики, 2022 г.
6. Онлайн-демонстрация «1С:Бухгалтерии 8» [Электронный ресурс]. URL:https://v8.1c.ru/buhv8/online-demonstraciya (дата обращения: 26.07.2023).

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 159.9.01

СИГНИФИКАТИВНО-ДЕНОТАТИВНЫЙ ПЕРЕНОС В ТЕХНОЛОГИИ МАНИПУЛЯЦИИ СОЗНАНИЕМ

Беломестнова Нина Васильевна
Ленинградский государственный университет им. А.С. Пушкина
196605, г. Санкт-Петербург, Пушкин, Петербургское шоссе, д.10
e-mail: belomestnovanina@bk.ru

Аннотация. Описывается технология сигнификативно-денотативного переноса в средствах воздействия на сознание субъекта при манипуляции с целью извлечения односторонней выгоды (обмана). Знание семантического треугольника Г. Фреге позволяет человеку защитить свою психологическую безопасность.

Ключевые слова: семантический треугольник Г. Фреге; технологии манипуляции сознанием; структура и механизмы психики и сознания.

SIGNIFICATIVE DENOTATIVE TRANSFER TO MIND MANIPULATION TECHNOLOGY

Belomestnova Nina
Pushkin Leningrad State University
10 Petersburgskoye shosse, St. Petersburg, 196605, Russia
e-mail: belomestnovanina@bk.ru

Abstract. The technology of significative-denotative transfer in the means of influence on the consciousness of the subject when manipulating with the purpose of unilateral benefit (deception) is described. The knowledge of G. Frege's semantic triangle allows the individual to protect his psychological security.

Keywords: G. Frege's semantic triangle; consciousness manipulation technologies; structure and mechanisms of psyche and consciousness.

Сигнификативная природа сознания человека дала ему разум, чтобы познавать суть вещей, скрытую от внешнего наблюдения, но и дала мощное средство сокрытия этой истинной сути, если один из сокоммуникаторов желает обмануть другого.

Идея знака как орудия мысли человека впервые была выдвинута Дж. Локком и поддержана Г. Лейбницем, но под «знаком» они имели ввиду математические и иные символы. Дальнейшее развитие понятия «знак» привело к пониманию слов человеческого языка как знака, а затем и к расширению этого понятия до сигнальной (знаковой) природы психики в советской психологии. Л.С. Выготский заявил идею слова как орудия человеческой мысли. Но слово возникло в биологической процессе эволюции регуляторных систем организма.

В эволюции живого организма-гетеротрофа последовательно возникали системы регуляции, отличающиеся кодом и его носителем. Диффузная нейро-иммунно-эндокринная [1-3] и ответившиеся от неё иммунная и эндокринная регуляторные системы в качестве кода используют молекулу конкретного вещества (медиатора). Нервная регуляторная система применяет в качестве кода нервный импульс (электрический импульс), а его носителем выступает нейрон. Затем в процессе эволюции на основе нервной появляется первый вариант психической системы регуляции – сенсорная психика, где кодом выступает сенсорный сигнал, а его носителем функциональная система нейронов. При появлении неокортекса психическая система регуляции стала перцептивной с кодом в виде перцептивного сигнала (образа-восприятия) и тем же носителем, а с эволюцией третичных полей неокортекса возникла, и репрезентативная система психической регуляции с кодом в виде образа-репрезентанта (образа-представления). В настоящее время вершиной в эволюции регуляторных систем организма является сознание, которое оперирует кодом-словом, носителем которого является целостный головной мозг человека в его функциональной асимметрии [4]. Кодовая природа психики исследовалась в санкт-петербургской школе психологии [5]. Слово является фундаментальным системообразующим для сознания человека феноменом, поэтому это одно из самых эффективных средств воздействия на сознание человека.

Но если коды всех предыдущих регуляторных систем организма являются простыми триггерами для запуска ряда реакций, то само слово не является простым звуком или несколькими графическими штрихами, которые выполняют роль триггера. Слово имеет сложный состав. Фердинанд де Соссю́р выделил в слове две составляющих – десигнат (обозначающее, внешняя форма слова) и денотат (само означенное явление). Го́тлоб Фре́ге разделил обозначенное явление (предмет, обозначенный словом) на собственно денотат (предмет) и

коннотат (смысл), указав, что один и тот же предмет может иметь разный смысл для разных людей. В результате слово обрело тройной «состав», или три аспекта, которые позже назвали семантическим треугольником Фреге. Три аспекта слова – сигнификат (форма слова), денотат (реальный материальный или идеальный объект, который сигнификат обозначает) и коннотат (конкретный смысл в данном контексте или для данного человека) – оказались средством не только творческого приёма в дискурсе или логическом анализе, но и возможностью манипуляции человеческим сознанием, то есть извлечением односторонней выгоды в процессе коммуникации.

Какие приёмы манипуляции сознанием выросли из треугольника Фреге?

Коннотат (в особенности его эмоционально-оценочная сторона) является средством техники, известной в психотерапии как «присоединение». Человек, желающий вызвать доверие у своего собеседника, предъявляет такие же коннотации в обсуждаемой теме, как и у его визави. Второй собеседник начинает чувствовать общее «мировидение», общность мировоззрения, принципов бытия, морально-этических оценок, что позволяет первому сокоммуникатору в какой-то момент начинать предъявлять те идеи, которые позже приведут его визави к материальной или моральной потере, то есть к обману.

Так же действует и явление, которое мы назвали сигнификативно-денотативный перенос. Весьма часто сигнификат (собственно звучащее или написанное слово) имеет несколько денотатов. Слово «фирма» большинством обывателей воспринимается как организация, производящая какую-либо продукцию, а слово «сотрудник» воспринимается как человек, трудоустроенный в этой «фирме», выполняющий определённую функцию и получающий за это заработную плату. Но позже выясняется, что под «фирмой» имелся ввиду благотворительный фонд, а «сотрудники» – это пожертвователи в этот фонд. В этом примере узнаётся один из приёмов так называемых «пирамид» и «семинаров», осуществляющих рекрутинг новых жертв мошенничества.

Иногда смена денотата при одном сигнификате происходит стихийно, в живом коммуникативном процессе, без осознанной цели обмана. Например, до 1990 годов XX века выражение «традиционная медицина» применялось для народной, «травной», «целительской» помощи при заболеваниях, а собственно современная медицина именовалась «научной» или «современной» медициной. В XXI веке денотаты инвертировались. Теперь научно-обоснованная медицина именуется «традиционной», а народная называется «альтернативной».

В психологии XX века термин «жизнедеятельность» применялся для обозначения биологических процессов в организме, а личностные трансформации и смысложизненные преобразования назывались «личностной деятельностью», «социальной деятельностью». В XXI веке, развернувшем психологию от естественнонаучного подхода к духовным практикам и личностно-смысловым поискам, довольно быстро именно личностные поиски стали называться «жизнедеятельностью», что нередко вносит недопонимание в дискуссии специалистов разных научных школ и поколений.

Таким образом, знание треугольника Фреге может помочь человеку в противостоянии попыткам обмануть его сознание.

СПИСОК ЛИТЕРАТУРЫ

1. Kvetnoy I.M. Extrapineal melatonin: location and role within diffuse neuroendocrine system // The Histochemical Journal 31: 1-12. 1999.
2. Акмаев И.Г. Взаимодействие нервных, эндокринных и иммунных механизмов мозга // Журнал невропатологии и психиатрии им .С.С.Корсакова, 1998. N 3. С. 54-56.
3. Акмаев И.Г. Современные представления о взаимодействиях регулирующих систем: нервной, эндокринной и иммунной //Успехи физиологических наук, 1996. Т.27. №1. С. 3-20.
4. Беломестнова Н.В. Уровни знаковой регуляции (от простейших до человека) // Психология человека: интегративный подход. Сб. статей / под ред. д. пс.н., проф. В.Н.Панферова. – СПб.: Изд-во АНО «ИПП», 2007. – С. 15-35.
5. Веккер Л.М. Психические процессы. – Л.: ЛГУ, том 1,1974, 335с.; том 2, 1976, 343 с.; Том 3. 1981. – 327 с.

УДК 323.2

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННО-ПОЛИТИЧЕСКОМУ ВОЗДЕЙСТВИЮ НА ДОЛЖНОСТНОЕ ЛИЦО

Борщенко Виктор Владимирович
Северо-Западный институт управления – филиал РАНХиГС
Средний пр. В. О., 57, Санкт-Петербург, 199178, Россия
e-mails: boss-victor@yandex.ru

Аннотация. Статья посвящена анализу способов влияния на должностных лиц и методов противодействия. В качестве метода противодействия рассматривается сценарное моделирование. Представлены различные виды сценариев и их использование в проблемных ситуациях.

Ключевые слова: Информационно-политические риски; информационное пространство; защищенность информационно-политической среды; методы политического манипулирования; сценарное моделирование; информационно-политическое воздействие.

METHODS OF COUNTERING INFORMATION AND POLITICAL IMPACT ON AN OFFICIAL

Borshenko Viktor
Northwestern Institute of Management - branch of RANEPA
57 Sredny Av. V. I., St. Petersburg, 199178, Russia
e-mails: boss-victor@yandex.ru

Abstract. The article is devoted to the analysis of ways to influence officials and methods of counteraction. Scenario modeling is considered as a countermeasure method. Various types of scenarios and their use in problem situations are presented.

Keywords: Information and political risks; information space; security of the information and political environment; methods of political manipulation; scenario modeling; information and political impact.

Информационно-политические риски и угрозы являются развивающимися процессами использования методов политической манипуляции. Их цель: создание у объектов манипуляции необходимых взглядов на социально-политическое развитие страны.

Так, если технология информационно-политического воздействия направлена на значимое высокопоставленное должностное лицо, то она должна учитывать: специфику его характера и образа жизни; возможность влияния на это лицо в процессе его контактов с высокопоставленными представителями государств-конкурентов на официальных мероприятиях и в ходе частных встреч; степень участия этого лица в информационном пространстве в целом и в интернет-пространстве, в частности, на официальном и личном уровне; степень доверия к должностному лицу при осуществлении им своих обязанностей; уровень взаимоотношений должностного лица с системной и несистемной оппозицией и его представление в информационном пространстве; наличие близкого окружения, способного влиять на принятие управленческих решений; наличие в стране событий отрицательного характера; произошедшие техногенные катастрофы; недостаточное нормативное обеспечение деятельности должностных лиц в сфере национальной безопасности.

Кроме того, должны быть рассмотрены связи этого должностного лица с другими информационно-критическими элементами политической структуры и выявлена потенциальная степень влияния этих элементов на рассматриваемое должностное лицо.

Наличие этих свойств позволяет выделить три-четыре основных взаимосвязанных направления информационно-политического воздействия при формировании и реализации угрозы «навязывания неприемлемых стандартов в развитии демократического общества» в части смены его руководства:

– Информационно-политическая атака на само должностное лицо;

– Информационно-политическая атака на его близкое окружение (родственники, друзья, соратники);

– Информационно-политическая операция в отношении тесно связанных с должностным лицом информационно-критических элементов политической структуры;

– Информационно-политическая операция в отношении населения страны.

В процессе реализации информационно-политических технологий в интернет-пространстве используют как открытые виды информационно-политической манипуляции, так и методы скрытых манипуляций с целью побуждения к действиям различного рода. Выделим три группы информационных признаков:

– информационные признаки открытого информационного воздействия на все элементы политической структуры по всем рассмотренным направлениям. Эти признаки могут быть определены путем смыслового анализа информационных контентов, появляющихся в открытой части интернета;

– информационные признаки, отражающие результаты скрытого информационно-политического воздействия. Эти признаки могут быть определены двумя способами, во-первых, путем анализа скрытой части интернета («глубокая зона» — это тысячи страниц интернета, которые скрыты от индексации поисковых систем, а попасть на них можно только с зашифрованных интернет-соединений), во-вторых, по результатам деятельности должностного лица после его плановых официальных или частных контактов с представителями конкурирующих государств;

– информационные признаки, соответствующие общим результатам информационно-политического воздействия. Эти признаки могут быть разработаны путем анализа текущего состояния общественно-политической обстановки в стране и ее освещении в интернете.

Основу моделирования подобных процессов составляет теория сценариев. На её основе создаются логически связанные (гипотетические) последовательности событий. Данная теория даёт возможность определять конкретные варианты развития информационно-политических рисков и угроз. Также, давать качественную или количественную оценку возможных альтернативных вариантов их реализации [1].

К основным видам сценариев следует относить следующие: вербальные сценарии, фрейм-сценарии, веера вариантов (решений, концепций), информационно-признаковые модели.

Как исходные данные для построения сценариев можно использовать:

наличие проблемной ситуации (экономической, политической, или другой), включающей все необходимые данные для принятия решений об общем характере сценария (оптимистический, сохранение статус-кво или пессимистический), а также для детальной разработки его отдельных этапов и элементов; конкретный и поэтапный план действий, направленных на ее скорейшее разрешение.

Указанные исходные данные широко применяются для выявления стандартных сценариев развития рисков и угроз.

В известных методах сценарного моделирования слабо учитывается влияние состояния информационной среды на процесс формирования и развития этих угроз в целом, а также не рассматривается зависимость состояния акторов от информационного воздействия. Кроме того, типовые модели требуют их адаптации к конкретной общественно-политической обстановке, особенностям политических взглядов различных слоев

населения, социальных групп, государственных, политических и общественных деятелей, в том числе их индивидуальных свойств.

Вместе с тем, в известных подходах есть ряд методологических приемов, комплексное применение которых позволяет на их основе построить новую общую технологию сценарного моделирования информационно-политического воздействия (манипулирования), учитывающую информационный фактор в процессе формирования и развития угрозы. Эта технология представляет собой взаимосвязанную реализацию следующих модельных блоков: «структура информационно-политической угрозы», «политическая структура», «определение информационно-критических элементов политической структуры», «операционно-временная модель информационно-политического воздействия», «оценка текущего состояния информационно-политического воздействия.

Таким образом, информационно-политическое воздействие в интернете может быть представлено в виде четырех основных моделей.

Первая модель предусматривает воздействие на отдельных политических деятелей, оказывающих значимое влияние на политическую систему страны. Структура информационно-политической угрозы при этом предусматривает формирование у пользователей представления об этом акторе, как угрозе их благополучию или политической системе государства. Актор, в отношении которого осуществляется манипуляция, позиционируется как исключенный из политической системы или как включенный в политическую систему угрожающей системы (например, как иностранный агент). Любая его деятельность рассматривается как приносящая вред социально-экономическому развитию данного государства в случае, если такого негативного результата не находится, представляются экспертные заключения о возможном скрытом негативном воздействии. При публикации компрометирующей информации чрезвычайно важен временной аспект, так как воздействие должно осуществляться постоянно и по нарастающей [2]. Оценка текущего состояния информационно-политического воздействия осуществляется посредством определения рейтинга данного политического актора.

Вторая модель предусматривает воздействие на значимые общественно-политические объединения, например, религиозные организации. Основной угрозой в данной модели чаще всего представляется угроза общечеловеческим ценностям — свободе слова, свободе вероисповедания, толерантность и т.п. Активно публикуется информация, подтверждающая влияние объединения, в отношении которого осуществляется манипуляция, на формирование политической структуры или на акторов, включенных в эту структуру. Такой информацией могут быть как визуальные доказательства, так и экспертные оценочные утверждения. Активность объединения рассматривается в негативном аспекте, например, благотворительные мероприятия могут трактоваться как рекрутинговые акции или как имитационная деятельность («подарки получили только дети, являющиеся членами семей сектантов»). По сравнению с первой моделью появляется дополнительный манипуляционный механизм — стигматизация. Определяется максимально негативный образ, включающий как отталкивающие внешние черты, так и отрицаемое сообществом поведение, с которым впоследствии ассоциируется любой участник объединения. Операционно-временной блок предусматривает периодическое воздействие, так как постоянное размещение информации играет скорее информационную роль и может, напротив, вызвать эффект привыкания, а затем и вызвать интерес к дискредитируемому объединению. Так, например, произошло с протестантской церковью, в отношении которой католическая церковь вела активные информационные войны, единственным результатом которых стало повышение узнаваемости догматов протестантизма и рост симпатий к нему среди населения. Оценка эффективности воздействия в данном случае осуществляется по критерию узнаваемости объединения и контекста его упоминаний. Наиболее целесообразным методом оценки манипулятивного воздействия в этой модели является контент-анализ [3].

Третья модель предусматривает воздействие на отдельные социально-демографические группы. В качестве угрозы в данном случае выступает традиционный страх «чужого», социально-культурные различия гипертрофируются. Особенное значение придается потенциальному включению представителей этой группы в состав правящей элиты и трансформации ценностей политической структуры в соответствии с ценностями этой группы. Любые акторы, в отношении которых манипулятор отмечает общественное недовольство, ассоциируются с угрожающей социально-демографической группой, что призвано усилить недовольство именно этой группой [4]. Активно используется механизм стигматизации, причем в наиболее примитивном его виде — выдумываются прозвища, одновременно обидные и вызывающие смех, их основой чаще всего являются особенности внешнего вида или непонятные культурные традиции [5]. По временной шкале воздействие осуществляется так же, как и в первой модели, постоянно, например, придуманные прозвища употребляются в любом обсуждении, в котором упоминается дискредитируемая социально-демографическая группа. Оценка эффективности воздействия в данной модели подразумевает определение ассоциативного ряда, с которым связывается в представлении пользователей сети данная группа, что подразумевает использование более сложных комбинированных методов исследования.

Наконец, четвертая модель подразумевает воздействие на официальные информационные ресурсы. Основной угрозой, как и во второй модели, в данном случае признается влияние на общечеловеческие ценности. Основным фактором манипуляции становится достоверность информации, предоставляемой государственными СМИ. Так же, как и в первой и второй моделях, любая информация, предоставленная через этот канал, подвергается сомнению или напрямую определяется как ложная. В противовес предоставляются ложно-

достоверные свидетельства, источниками которых могут быть как добросовестно заблуждающиеся свидетели, так и откровенно недостоверные слухи. В некоторых случаях источником дезинформации становится сам манипулирующий субъект, хотя такое развитие событий нежелательно, так как нарушает принцип скрытности манипуляции. Причиной ложности информации всегда определяется политическая ангажированность официального СМИ. Требование к оперативности манипуляционного воздействия в четвертой модели является определяющим, так как бывает эффективным только в случае появления дискредитирующей информации сразу же после публикации официальной. Оценка результативности воздействия осуществляется посредством определения уровня доверия к информации, предоставляемой государственным СМИ, что в силу субъективности понятия доверия также требует комплексного подхода.

Итак, модели информационно-политической манипуляции, разработанные на основе сценарного подхода, позволяют определить признаки манипуляции до того, как будет причинен значимый ущерб социально-политической структуре государства и оказать адекватное противодействие.

СПИСОК ЛИТЕРАТУРЫ

1. Манойло А. В. Государственная информационная политика в особых условиях: Монография. М. : МИФИ, 2003. 388 с.
2. Proto L. Who's pulling your strings? How to stop being manipulated by your own personalities. Wellingboroug: Thorsons. 1989. P. 53.
3. Бухарин С. Н. Методы и технологии информационных войн. М. : Академический проект, 2007. 384 с.
4. Володенков С. В., Митева В. В. Сетевые информационные войны в современных условиях: основные акторы и стратегии // PolitBook. 2016. № 3. С. 18–35.
5. Максимова А.Б. Язык в интернет-коммуникации: общие закономерности и национально-культурные особенности (на материале русского и английского языков) // Вестник РУДН. Серия: Теория языка. Семиотика. Семантика. 2010. № 3. С. 74–90.

УДК 001.2; 004.81; 004.946

СОЦИОКУЛЬТУРНАЯ ТРАНСФОРМАЦИЯ УКРАИНСКОГО ОБЩЕСТВА: АЛЬТЕРНАТИВНЫЕ КОНЦЕПЦИИ В КОНТЕКСТЕ ЭВОЛЮЦИОННЫХ И ЦИКЛИЧНЫХ ТЕОРИЙ

Дегтярева Ольга Викторовна
Северо-Западный институт управления – филиал РАНХиГС
Средний просп. В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: olgaspb2008@mail.ru

Аннотация. В работе анализируются такие альтернативные теории развития украинского общества в транзитивный период, как: Украина как виртуальное общество; Украина как вирусное общество; Украина как «сателитное» общество; Украина как общество стойкого развития; Украина как постмодернизационное общество.

Ключевые слова: Украина; трансформация; детрадиционализация; «сателлитное» общество.

SOCIOCULTURAL TRANSFORMATION OF UKRAINIAN SOCIETY: ALTERNATIVE CONCEPTS IN THE CONTEXT OF EVOLUTIONARY AND CYCLICAL THEORIES

Degtyareva Olga
Northwestern Institute of Management - branch of RANEPA
57/43 Middle Ave. V.I., St. Petersburg, 199178, Russia
e-mail: olgaspb2008@mail.ru

Abstract. The article analyzes such alternative theories of development of the Ukrainian society in the transitive period as: Ukraine as a virtual society; Ukraine as a viral society; Ukraine as a «satellite» society; Ukraine as a sustainable development society; Ukraine as a post-modernization society.

Keywords: Ukraine; transformation; detraditionalization; «satellite» society.

Процессы, которые происходят в современной Украине, не могут быть истолкованы в рамках существующих теорий модернизации, постмодернизации и других., поскольку современное украинское общество решает одновременно и параллельно задачи нескольких периодов. При таком положении вещей наблюдаются не только прогрессивные изменения, а и элементы регресса, есть признаки консервативного отступления и традиционных явлений. Соответственно, понимание этих процессов вынуждает исследователей искать такое теоретическое осмысление, которое бы учитывало противоречивость наблюдаемых процессов. Представляется, что такой теорией может выступить теория трансформации. При этом следует учитывать и ставить задачу более полной разработки этого подхода для того, чтобы соотнести положения теории с существующими концепциями социального развития в Украине, рассмотреть последствия в контексте положений других теорий общества, которые внедряются в украинском дискурсе. В работе рассмотрены основные альтернативные концепции построения украинского общества, а именно:

– Украина как виртуальное общество;
– Украина как вирусное общество;
– Украина как «сателлитное» общество;
– Украина как общество стойкого развития;
– Украина как постмодернизационное общество;

В связи с этим, динамика социальной структуры, смена экономического, политического, правового, экологического сознания, ценностных ориентаций, новых явлений в образе жизни, потребительском поведении украинцев требует теоретического осмысления и эмпирического подтверждения положения теорий [1]. Термин «трансформация» рассматривается не просто как синоним терминов «развитие», «преобразования», «изменения», «модернизация» и т.п., а как самостоятельная социологическая категория теории социального развития. Эта категория описывает особенное положение общества, при котором происходят качественные изменения формы социальных связей, типов и способов развития.

В работах российских и украинских исследователей распространена точка зрения, согласно которой модернизация в постсоветских государствах носит запоздалый характер [2]. В ряде работ рассматриваются характерные черты переходного периода, в частности, разрушение системы ценностей, социокультурная дестабилизация, моральный ригоризм, возрождение сакрального, изменение критериев социальной структуры, превращение культуры в фактор, который определяет социальную жизнь, обострение нетолерантного отношения к «другому», отрыв культурных традиций от социально-исторических ориентиров, детрадиционализация и прочие расхождения. В работах Э. Этциони, П. Бергера, Ш. Айзенштадта раскрываются закономерности модернизации, которая выступает чертой транзитивного общества.

Характерной чертой трансформирующегося общественного правосознания выступает аномия. В кризисном обществе проблема аномии поднимается до уровня центральной в регулировании нарушений общественного взаимодействия. Этот термин применяется для характеристики положения общества, при котором для большинства снижается значение социальных норм, что является причиной девиантного поведения. Аномия также характеризует утрату социальной идентификации, которая порождает деклассированное положение [4]. Люди перестают идентифицировать себя с определенной социальной группой, теряют чувство социальной солидарности. В общественно-политической сфере аномия сопровождается усилением авторитаризма, политического экстремизма и этноцентризма. Социальная аномия представляет собой особое нравственно-психологическое состояние сознания, характеризующееся вакуумом идеалов и разложением моральных ценностей. Понятие «аномия» раскрывает явление, вполне соотносимое с пониманием социального хаоса, возникающего при радикальных трансформациях обществ – когда прежние нормы перестают действовать, а новые не образовались.

Проблема идентификации является стержневой в национальной сфере. В СССР проводилась политика снижения значения национальной идентификации людей. Значение принадлежности к нации в метарегионе Восточной Украины было небольшим [3]. Язык не является обязательным фактором национальной самоидентификации. Большую роль играет национальность родителей, проживание на украинской территории, воспитание. Трансформация в этой сфере сознания совершается в направлении формирования национально-государственной идентичности.

Что касается религиозной сферы, то здесь следует обратить внимание на наличие двух типов традиций: недавнего и отдаленного прошлого. В зависимости от актуализации того или иного типа традиций религиозные верования имеют консервативный или модернизационный импульс. Если акцентируется давняя, например, досоветская традиция, церковь начинает играть модернизационную роль. Обновление духовной жизни через, например, изменение дат и названий церковных праздников, что воспринимается как модернизация, включает процесс обновления религиозного сознания в той форме, которая была свойственна обществу досоветского времени.

Социокультурная трансформация предусматривает изменения контекста восприятия реальных событий [5]. Изменяется содержание преобразований. Если М. Вебер выявлял трансформационные явления в культуре с помощью анализа религиозного сознания, то в настоящее время целесообразнее обратить внимание на тенденции, например, в музыкальных жанрах. Изменение культуры влечет за собой изменения инструмента и объекта анализа этой культуры.

СПИСОК ЛИТЕРАТУРЫ

1. Смерічевський С. Ф., Полоус О. В. Трансформація економічних процесів в контексті глобалізаційних зрушень // Науковий вісник Ужгородського нац. ун-ту. Серія: Міжнародні економічні відносини та світове господарство. Ужгород: Вид. дім «Гельветика», 2018. С. 142–148.
2. Танчер В., Карась О., Кучеренко О. Політичні партії та рухи у світлі «ситуації постмодерну». К., 1997. С. 4-5.
3. Хартія регіоналізму [Электронный ресурс]. URL: http://fssembly.coc.int/nw/xml/xref/xref-DokDetaslsEN.asp?fileid=175820@lang (дата звернення – 27. 05. 2021).
4. Євдокімова О.О. Інформаційно-психологічні впливи в умовах соціальної аномії // Право і безпека., 2015. № 4 (59). С. 6-10.
5. Євдокимова О. О. Реакції бойового стресу, гострі та віддалені, як наслідок АТО // ІІІ Всеукраїнський психологічний конгрес з міжнародною участю «Особистість у сучасному світі»: зб. наук. пр.. К.: Інформац.-аналіт. агентство, 2014. С. 217–223.

УДК 001.2; 004.81; 004.946

ТЕХНОЛОГИИ КОГНИТИВНОЙ БЕЗОПАСНОСТИ НА ПУТИ ИНТЕГРАЦИИ

Кефели Игорь Федорович
Северо-Западный институт управления РАНХиГС при Президенте Российской Федерации
Средний просп. В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: geokefeli@mail.ru

Аннотация. Анализируются перспективы формирования системы технологий обеспечения когнитивной безопасности в рамках когнитологии, объединяющей исследования когнитивных процессов на основе объединения усилий философии, нейробиологии, психологии, лингвистики, антропологии и информатики.

Ключевые слова: когнитология; система когнитивных технологий; когнитивная война; когнитивная безопасность.

COGNITIVE SECURITY TECHNOLOGIES ON THE WAY OF INTEGRATION

Kefeli Igor
North Western Institute of Management RANEPA under the President of the Russian Federation
Middle Ave. V.O., 57/43, St. Petersburg, 199178, Russia
e-mail: geokefeli@mail.ru

Abstract. The prospects for the formation of a system of technologies for ensuring cognitive security within the framework of cognitive science, which combines the study of cognitive processes based on the combined efforts of philosophy, neurobiology, psychology, linguistics, anthropology and computer science, are analyzed.

Keywords: cognitive science; system of cognitive technologies; cognitive warfare; cognitive security.

Междисциплинарный характер когнитивной науки (когнитологии) должны были придать совместные исследования шести отраслей знания: психологии, лингвистики, компьютерной науки, нейронауки, антропологии и философии. На протяжении второй половины XX века формировались различные направления когнитологии, в которой, к настоящему времени, усиливаются интегративные тенденции, направленные, в частности, на разработку когнитивных технологий с целью обеспечения когнитивной (ее еще называют ментальной) безопасности. Актуальность последней диктуется необходимостью принятия защитных мер в ответ на активные действия НАТО в концептуальном обосновании ведения когнитивных операций в формате нового домена гибридной войны – сознание человека, его чувства, мысли, душа, мировоззрение. Военным специалистам этого альянса предписано, в тесном сотрудничестве с научными кругами заниматься «милитаризацией наук о мозге» согласно правилу: «когнитивная война изменяет не только то, что люди думают, но и то, как они действуют» [1]. Первоочередные задачи отечественной науки, технологии и образования – это:

– теоретико-методологическое обоснование статуса когнитивной безопасности в контексте глобальной безопасности;

– разработка соответствующих когнитивных технологий обеспечения национальной безопасности России;

– подготовка кадров высшей квалификации по новому направлению «информационно-психологическая и когнитивная безопасность».

Вопросы, касающиеся технологий обеспечения когнитивной безопасности в рамках операционного пространства когнитологии, предполагают унификацию названия ее разделов: когнитивная философия, когнитивная нейробиология, когнитивная психология, когнитивная лингвистика, когнитивная антропология и когнитивная информатика.

Когнитивная философия, выполняя в системе когнитологии мировоззренческую функцию, нацелена на разработку технологий формирования общественного сознания, идеологии, соответствующей национальным интересам государства (в данном случае, России) и противодействия чуждой идеологии.

Когнитивная нейробиология, нацеленная на разработку технологий обеспечения когнитивной безопасности, в полной мере базируется на естественнонаучном материале конкретных исследований защитных структур и функций нейронов и нейронных сетей.

Когнитивная психология занимает, как и когнитивная нейробиология, ключевое положение в системе когнитивных технологий в силу своей высокой степени разработанности теоретического аппарата, технологий и методик.

Когнитивная лингвистика ориентируется на решение проблемы смысла сущего, оперируя множеством технологий и приемов манипулирования словом, речью, зрительными образами, мировоззрением. Но при этом необходимо учитывать, что идеальность социальна по своей природе и происхождению. Это форма вещи, но вне этой вещи и именно в деятельности человека, как форма этой деятельности» [2]. «Идеальное» выявляется и фиксируется в исторически сложившихся формах духовной культуры, представляет собой сферу явлений коллективно созидаемого людьми мира духовной и материальной культуры (в том числе в кибернетической инженерии), а также во всей совокупности звеньев социальной культуры (культуры человеческих отношений – моральных, эстетических, религиозных, правовых, политических).

Когнитивная антропология в контексте когнитологии – междисциплинарная область знания, которая включает разделы социальной и культурной антропологии, связанные с интерпретацией знания, традиций представителей различных культур, а также исследующей когнитивные структуры, регламентирующие поведение, образ жизни людей, их восприятие мира. Когнитивная антропология, используя методы, когнитивной психологии и других разделов когнитологии (мозговое картирование, нейронные сети, дискурс-анализ и др.), создала возможности для формирования системы социальных технологий, которые могут найти применение в обеспечении когнитивной безопасности.

Когнитивная информатика предполагает решение проблемы соотношения искусственного и естественного интеллекта применительно к обеспечению когнитивной безопасности, опираясь на философскую категорию «идеальное». Выяснятся, что многими рисками, порожденными бурным прогрессом в сфере создания ИИ, озабочены не только представители гуманитарного знания, но и сами его разработчики: «Принципы работы в области ИИ» («AI principles»), принятые в 2017 г. на конференции в Асиломаре (Калифорния, США), «Глобальная инициатива IEEE по этике автономных и интеллектуальных систем» предполагают, что системы ИИ должны быть безопасны и разработаны таким образом, чтобы их функционирование было согласовано с человеческими ценностями, идеалами и культурным разнообразием. «Необходимо переосмыслить то, что мы подразумеваем под безопасностью, которую необходимо обеспечить с самого начала создания ИИ, в отличие от разработки надежной системы безопасности после» [3]. «Глобальная инициатива IEEE» представляет собой, пожалуй, первое детальное техническое руководство по этическим аспектам технологий автономных и интеллектуальных систем (Autonomous and Intelligent Systems, A/IS). Авторы данного руководства выдвинули ряд принципов проектирования, разработки и внедрения A/IS, основанных на этих моральных ценностях: благополучия (утверждение повышения благосостояния человека как основного критерия достижения успеха), эффективности (предоставление доказательств эффективности и пригодности A/IS), осознания возможного неправильного использования (защита от всевозможных злоупотреблений и рисков, связанных с использованием A/IS) и компетентности (опора на знания и навыки, необходимые для безопасной и эффективной работы) [4].

Пришло время, когда сами специалисты в области ИИ все более активно начинают выступать инициаторами гуманитарной экспертизы всего того, что связано с вычислительной техникой в целом и конкретно – искусственным интеллектом. В ежегоднике «Глобальные риски» (2019 г.) в числе одного из шоков будущего упоминается упомянутый выше «Цифровой паноптикум» (Digital panopticon), благодаря которому человечество движется в мир, где «все, что нас окружает, захватывается, сохраняется и подвергается алгоритмам искусственного интеллекта (ИИ)», а «геополитически будущее может частично зависеть от того, как общества с разными ценностями относятся к новым источникам данных». Более жестко прозвучали опасения по поводу экспансии ИИ в жизненный мир человека, обостряющей социальные риски в очередном докладе Давосского клуба 2020 года. Речь заходит о той «человеческой антиутопии», которая, учитывая растущую осведомленность общества о предвзятых (необъективных) алгоритмах и «киберзапугивании», взывает к более глубокому вовлечению этики в решение вопросов при разработке и использовании технологий ИИ, которые уже расцениваются не только как «самое впечатляющее изобретение» (приведшее, кстати, к манипуляции с помощью фейковых новостей и «глубоких фейков»), но и как «самая большая экзистенциальная угроза» [5].

Рассмотренный круг вопросов наводит на мысль о необходимости разработки системы когнитивных технологий, разрабатываемых в каждом из перечисленных выше разделов когнитологии с целью обеспечения когнитивной безопасности, о чем подробнее в коллективной монографии «Пролегомены когнитивной безопасности» [6]. Пришло время разработки и введения в действие, по словам советника Министра обороны Российской Федерации А. М. Ильницкого, «Стратегии ментальной устойчивости (безопасности) всего социума и отдельного индивида». Причем недавно этот ход размышлений Ильницкий развил, рассуждая об эффективности технологий когнитивной (ментальной) безопасности, обеспечивающих первичность идеологических и этических основ политики России в условиях цивилизационной войны с Западом [7].

СПИСОК ЛИТЕРАТУРЫ

1. Du Cluzel F. Cognitive Warfare. June-November 2020 // Innovation Hub (https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf).
2. Ильенков Э. В. Искусство и коммунистический идеал. Избранные статьи по философии и эстетике / вступ. статья М. Лифшица. М.: Искусство, 1984. С. 51-52.
3. Asilomar AI principles [Электронный ресурс]. URL: https://futureoflife.org/ai-principles/ (дата обращения: 11.01.2020); Conn A. Anca Dragan Interview [Электронный ресурс]. URL: https://future of life.org/2017/01/18/anca-dragan-interview/
4. The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Autonomous and Intelligent Systems, First Edition. IEEE, 2019. https://standards.ieee.org/content/ieee-standards/en/industryconnections/ec/autonomous-systems.html
5. The Global Risks Report 2019. 14th Edition. World Economic Forum Cologny. Geneva, 2019; The Global Risks Report 2020. 15th Edition. World Economic Forum Cologny. Geneva, 2020.
6. Пролегомены когнитивной безопасности. Коллективная монография / Под редакцией И. Ф. Кефели. – СПб.: ИД «Петрополис», 2023. – 488 с.
7. Ильницкий А. М. Стратегия ментальной безопасности России // Военная мысль. 2022. № 4; Ильницкий А. М. Война за государство // Международная жизнь. 2023. № 6.

УДК 001.2; 340.114.5

ПРАВОВЫЕ ОСНОВЫ КОГНИТИВНОЙ БЕЗОПАСНОСТИ

Кириленко Виктор Петрович, Алексеев Георгий Валерьевич
Северо-Западный институт управления РАНХиГС
199178, Россия, г. Санкт-Петербург, Средний пр. В.О., 57/43
e-mails: kirilenko-vp@ranepa.ru, deltafox1@yandex.ru

Аннотация. В условиях цифровой трансформации обеспечение когнитивной безопасности на универсальном, национальном и местном уровнях преследует одни и те же цели: защитить права человека и

обеспечить рациональность управленческих решений. Субъектом когнитивной безопасности всегда является индивид, уязвимый перед угрозой информационно-психологических операций. Когнитивная безопасность требует лидерских качеств от представителей политического руководства.

Ключевые слова: права человека; свобода слова; искусственный интеллект; массмедийное пространство, секьюритизация.

LEGAL BASIS FOR COGNITIVE SECURITY

Kirilenko Viktor Petrovich, Alekseev Georgy Valerievich
Northwestern Institute of Management RANEPA
199178, Russia, St. Petersburg, Sredny pr-kt V.O., 57/43
e-mails: kirilenko-vp@ranepa.ru, deltafox1@yandex.ru

Abstract. In the context of digital transformation, ensuring cognitive security at the universal, national and local levels pursues the same goals: to protect human rights and ensure the rationality of managerial decisions. The subject of cognitive security is always an individual who is vulnerable to the threat of information-psychological operations. Cognitive security requires leadership qualities from representatives of political leadership.

Keywords: human rights; freedom of speech; artificial intelligence; mass media space, securitization.

В соответствии с Конституцией Российской Федерации каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом; гарантируется свобода массовой информации; цензура запрещается (статья 29, части 4 и 5). В свою очередь, на государстве лежит позитивное обязательство по введению адекватных законодательной и административной основ, отвечающих требованиям ясности и определенности, для гарантирования эффективного плюрализма в средствах массовой информации и по поддержанию конкуренции в массмедийном пространстве. В соответствии с Законом Российской Федерации "О средствах массовой информации" учреждение средств массовой информации, владение, пользование и распоряжение ими не подлежат ограничениям, за исключением предусмотренных законодательством Российской Федерации о средствах массовой информации (ст. 1). На основании закона когнитивная безопасность обеспечивается в рамках либеральной парадигмы. Государство при этом осуществляет защиту граждан от проявлений насильственного экстремизма и деструктивной идеологии [2]. В Стратегии национальной безопасности Российской Федерации 2021 г. отмечается, что «стремление стран Запада сохранить свою гегемонию… сопровождаются обострением внутриполитических проблем, усилением межгосударственных противоречий, ослаблением влияния международных институтов и снижением эффективности системы глобальной безопасности» (п. 7). В стратегии отмечается, что «усиливающаяся нестабильность в мире, рост радикальных и экстремистских настроений могут привести к попыткам разрешить нарастающие межгосударственные противоречия за счет поиска внутренних и внешних врагов, к разрушению экономики, традиционных ценностей и игнорированию основных прав и свобод человека» (п. 8).В соответствии с Доктриной информационной безопасности Российской Федерации 2016 г. Информационная безопасность – «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства».

Расширение областей применения информационных технологий, создавая условиях для развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы [1]. Логика информационных войн провоцирует реалии экстремального политического процесса, где выход действий участников за пределы правового поля угрожает когнитивной безопасности граждан [3]. Состояние международного информационного пространства и угрозы информационных операций, направленных на разжигание русофобии и устранение России из общеевропейского политического процесса, отражают политизированность социально-гуманитарных наук и мифологизацию политики отдельных субъектов мировой политики. Россия последовательно выступает за «необходимость безотлагательного разрешения конфликта в региональном информационном пространстве» Европы, и за криминализацию тех политических технологий, которые дестабилизируют «информационное пространство, наносят вред репутации всех государств, вовлеченных в данное противостояние» [4 с. 20]. Разрешать значительную часть противоречий, лежащих в основе информационного конфликта в Европе, следует на основе учета совместных интересов и при объединении усилий для обеспечения информационной безопасности при уважении прав человека.

СПИСОК ЛИТЕРАТУРЫ

1. Пролегомены когнитивной безопасности. Коллективная монография / под ред. И. Ф. Кефели. – СПб.: ИД «Петрополис», 2023. – 488 с.
2. Алексеев Г.В., Аргылов Н.А., Байчик А.В., Бастрыкин А.И. и др. Глобальный индекс экстремизма. Санкт-Петербург, 2023. – 416 с.
3. Лабуш Н.С., Пую А.С. Медиатизация экстремальных форм политического процесса: война, революция, терроризм. СПбГУ. 2019. – 340 с.
4. Кириленко В.П., Алексеев Г.В. Политические технологии и международный конфликт в информационном пространстве Балтийского региона // Балтийский регион. 2018. Т. 10. № 4. С. 20-38.

УДК 316.6

МЕДИАОБРАЗ СОВРЕМЕННОЙ РОССИИ В СМИ ГРЕЦИИ

Кучинская Яна Францевна
Санкт-Петербургский государственный университет
Университетская наб. 7/9, Санкт-Петербург, 199034, Россия
st019442@student.spbu.ru

Аннотация. В статье представлены результаты контент-анализа европейской публицистики на примере газетных статей Греции. Частотный и тематический анализы текстов выявили модальность, содержательные акценты и приемы психологической манипуляции. В рамках международных отношений России и Украины выявлены приемы информационно-психологической войны для деформации не только образа России, но и образа всего русского мира.

Ключевые слова: медиаобраз, русский мир, контент-анализ, СМИ, Греция, манипуляция.

MEDIA IMAGE OF MODERN RUSSIA IN GREEK MASS MEDIA

Kuchinskaya Yana
Saint-Petersburg University
Universitetskaya nab. 7/9, St. Petersburg, 199034, Russia
st019442@student.spbu.ru

Abstract. The article presents the results of a content analysis of European journalism using the example of newspaper articles in Greece. Frequency and thematic analyzes of texts revealed modality, content accents, and methods of psychological manipulation. Within the framework of international relations between Russia and Ukraine, methods of information and psychological warfare have been identified to deform not only the image of Russia, but also the image of the entire Russian world.

Keywords: media image, Russian world, content analysis, mass media, Greece, manipulation.

«Русский мир» рассматривается как историческая общность людей, объединенных русским языком, культурой, исторической памятью, консервативными ценностями и морально-этическими нормами православия. На фоне сдвигов в международной политике, переустройства системы международных отношений и прокси войны, разжигаемой коллективным Западом, используются разнообразные приемы информационно-психологической войны для деформации не только образа России, но и образа всего русского мира [1] . Средства массовой информации дают, как правило, не чисто информационные материалы – конкретные факты, цифры, тексты тех или иных заявлений. Скорее, они порождают то, что можно было бы назвать информационными конструкциями [2].

С целью выявления актуальных идеологических акцентов, формируемых специфическими информационными конструкциями в европейской публицистике, был проведен контент-анализ официальных политических газетных интернет-изданий Греции – «Кафимерини» (пер. «Ежедневная»), «Вима» (пер. «Трибуна»), «Нафтэмборики» (пер. «Морская торговая»), с посещаемостью пользователей более 3 миллионов. Использовался частотный (более 50 000 знаков) и тематический анализ текстов (модальность, содержательные акценты, дискурс анализ, приемы психологической манипуляции).

Частотный анализ подтвердил повышенное внимание к политической повестке России и выявил многократное использование военной терминологии: война, вторжение, нападение, тоталитарное государство, как единственное средство описания СВО.

В процессе анализа текста (33 статьи) было выявлено упоминание стран и городов (всего 59). Наибольшее число упоминаний приходится на Россию (19,11%) и Украину (12,9%) – главные участники, Китай (7,69%) – важные участники и Запад (7,69%) от общего упоминания всех перечисленных стран выше.

Частотность упоминаний (94 единицы) российского президента В.В. Путина указывает на главенствующую роль этого участника в российско-украинских отношениях на фоне СВО. Особенно это актуально в сравнении с частотностью упоминания В. Зеленского - 3 единицы, что демонстрирует степень их политической веса.

В результате дискурс анализа греческих политических СМИ выявлены лингвистические средства построения образа России русского мира на фоне обострения российско-украинских отношений. Качественный анализ показал, что образ России как ядра русского мира представлен с отрицательной модальностью. Негативная окраска языковых единиц проявляется в субъективных интерпретациях, оценочных мнениях, с частым замалчиванием фактов и искажением событий. Был выявлен ряд манипулятивных приемов: навешивание ярлыков, высмеивание, предвосхищение событий в свою пользу, сравнение с отрицательными образами, использование военной терминологии в отношении объекта дискредитации, риторические вопросы, отрицательные исторические аналогии, гиперболизация и обесценивание. Реже используется ирония как сопровождающая политический нарратив технология дискредитации, инструмент искажения смыслов, действий и образов. Принцип противопоставления России Западу усиливает поляризацию формируемых образов, где эффект убеждения достигается не столько посредством эмоционально окрашенных характеристик, сколько описательной лаконичностью таких понятий как единство, единодушие, благополучие, альтруизм Запада в

борьбе против России во имя спасения остального сообщества стран. Нарочитое подчеркивание схожести судьбы релакантов с беженцами, создает критерий принадлежности российского гражданина к русскому миру. Таким образом, деление россиян по принципу согласия или несогласия с государственной политикой достигается путем выпячивания противопоставления граждан, с одной стороны, президента и правительства России, с другой стороны, разобщая русский мир посредством стилистических средств. В качестве контрмер необходимо использовать информационные противовесы и способствовать русской консолидации. В условиях глобализации обеспечить национальную безопасность, при которой сохраняется целостность России и возможность быть самостоятельным субъектом системы международных отношений [3].

СПИСОК ЛИТЕРАТУРЫ

1. Дейнека О.С. Образ и медиаобраз России в сознании немецких граждан на фоне усиления радикальных установок в обществе // Общество: социология, психология, педагогика. 2021. № 12. С.225-231.
2. Мезенцев Д. Ф. Психологическое воздействие информационных фантомов // Вестник политической психологии. 2002. №1 (2).
3. Кефели И.Ф. Судьба России в глобальной геополитике. - СПб.: Изд-во Северная звезда, 2004.

УДК 304.444

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В МЕДИЙНОЙ СФЕРЕ: ПРОГРЕСС ИЛИ УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?

Лай Линчжи
Санкт-Петербургский государственный университет
Университетская наб.,7-9, Санкт-Петербург, 199034, Россия
e-mail: 1169478672@qq.com

Аннотация. В статье дан критический анализ исследований, фиксирующих влияние искусственного интеллекта на производство новостей и медиапотребление. Поднимается проблема оценки информационных рисков при внедрении ИИ в журналистскую практику.

Ключевые слова: информационный кокон; информационная безопасность; искусственный интеллект; производство новостей.

ARTIFICIAL INTELLIGENCE IN THE MEDIA SPHERE: PROGRESS OR A THREAT TO INFORMATION SECURITY?

Lai Lingzhi
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: 1169478672@qq.com

Abstract. The article provides a critical analysis of studies that document the impact of artificial intelligence on news production and media consumption. The problem of assessing information risks when introducing AI into journalistic practice is raised.

Keywords: information cocoon; Information Security; artificial intelligence; news production.

В последние годы применение искусственного интеллекта (ИИ) в работе становится не случайной практикой отдельных СМИ, а широко распространенным явлением в медиаиндустрии, медиаобразовании, медиапотреблении, что находит отражение в научном дискурсе [1-3]. Такие программы ИИ, как ChatGPT, GPT-3 или DALL-E способны копировать когнитивную систему человека, влияя на эффективное и быстрое обучение решению логических и познавательных задач [18]. С обновлением и итерацией алгоритмической технологии масштаб применения искусственного интеллекта в сфере журналистики также постоянно расширяется. В медийной сфере это дает возможность повысить эффективность написания новостей. В то же время, принимая во внимание необходимость обновления последних данных, особенно при публикации внезапно происходящих и срочных новостей в режиме реального времени, применение искусственного интеллекта намного экономит время и труд сотрудников редакции.

Диалоговая (интерактивная) журналистика» — это новая форма применения искусственного интеллекта в журналистике. Например, во время новой коронавирусной эпидемии в 2020 г. Би-би-си запустила новостной чат-бот BBC Corona Bot. Пользователи могут вводить ключевые слова для вопросов в чате, чтобы одним щелчком мыши получать динамическую информацию в режиме реального времени, связанную с эпидемией в любом городе Великобритании. Существуют в основном два направления использования технологии искусственного интеллекта для повышения новостной интерактивности: во-первых, для представления большего объема информации более кратким и удобным интерактивным способом и оптимизация эффекта широкомасштабного распространения информации; во-вторых, для точного определения потребностей пользователей и своевременного совершенствования метода взаимодействия пользователей благодаря анализу пользовательских данных. Несмотря на очевидные удобства и преимущества использования искусственного интеллекта, его применение обесценивает труд журналиста и таит в себе значительные угрозы традиционным журналистским

ценностям. Это не может не отражаться на потребителях медиапродукта и информационном обмене. В связи с чем актуализируются проблемы определения рисков внедрения ИИ в медийную практику.

При применении искусственного интеллекта корреляция больших данных заменяет причинно-следственную связь в качестве новой системы логической интерпретации. Как было замечено ранее, автоматизация написания создания с использованием искусственного интеллекта повышает эффективность новостного производства и снижает трудозатраты. Однако роботизация в медийном производстве создает информационный кокон интенсивного уровня. Механизм абстрактной фильтрации рекомендует конкретным пользователям и аудитории информационные сообщения, которые автоматически генерируются машиной, но журналисты не могут вмешиваться в этот процесс. Закрытие «информационного кокона» напрямую бросает вызов публичности, которая считается нормой в традиционных журналистских ценностях. В данном случае написание новостей с помощью искусственного интеллекта делает журналистские ценности алгоритмизированными. Кроме того, как показывают опросы работников медиакомпании, они со скептицизмом относятся к данному направлению, так как «ответственность остается на плечах журналиста не только из-за уязвимости в российских реалиях алгоритма, который разработчики пока не могут довести до релевантного уровня выполнения работы, и недоверия журналистов к направлению, но и из-за отношения к алгоритму как к инструменту, с помощью которого человек может упрощать свою работу» [4].

Технология искусственного интеллекта позволяет медиаплатформам, полагающимся на новые технологии, удовлетворять собственные коммерческие интересы во имя удовлетворения общественной информационной потребности. Возьмем в качестве примера китайского новостного и информационного и мобильного приложения Jinri Toutiao, рекомендующего персонализированную информацию для индивидуальных пользователей на основе технологии искусственного интеллекта.

Пользовательские предпочтения и приоритет самой платформы являются важным элементом, составляющими ценность опубликованных новостей. За вызовом применения искусственных технологий традиционным журналистским ценностям стоит изменение существующего механизма распределения полномочий. При применении искусственного интеллекта незаметно происходит новый виток иерархического разделения. Новые медиаплатформы, использующие искусственный интеллект, обладают огромными информационными ресурсами благодаря тесной связи между искусственным интеллектом и большими данными.

Большие данные, естественно, включают в себя личную информацию о конфиденциальности аудитории. Применение в медийной сфере искусственного интеллекта нередко стирает границы между конфиденциальностью и данными, что делает последние уязвимыми.

В нынешнем контексте, когда речь идет об искусственном интеллекте, слову «интеллекту» уделяется достаточно внимания, в то время как слово «искусственное» отошло на второй план. Стоит упоминать, что цифровые алгоритмы написаны человеком. Значение этого факта заключается в том, что человек по логике должен обладать абсолютной инициативой в вопросе функционирования искусственного интеллекта. Искусственный интеллект не заменяет интеллект до конца, раз он искусственно создан человеком. Однако же на нынешнем этапе стоит практическая задача, как заставить искусственный интеллект служить журналистике, не поколебав традиционные журналистике ценности, не поколебав статус человека в качестве главного субъекта, и как не создать угрозу информационно-психологической безопасности личности, на которую направлен роботизированный медиапродукт.

СПИСОК ЛИТЕРАТУРЫ

1. Pavlik J. V. Collaborating With ChatGPT: Considering the Implications of Generative Artificial Intelligence for Journalism and Media Education, Journalism & Mass Communication Educator. 2023.
2. Shilina M. G., Wirth J. Immersive technologies in media: towards the concept of generative mediatization? RUDN Journal of Studies in Literature and Journalism. 2021. V. 26. 4. Pp. 673-680.
3. Shin D., Al-Imamy S., Hwang, Y. Cross-cultural differences in information processing of chatbot journalism: chatbot news service as a cultural artifact. Cross Cultural & Strategic Management. 2022. V. 29. № 3. Pp. 618-638.
4. Исаев Е. М., Кокорева М. В. Роботизация новостной журналистики в России: новые принципы работы и трансформация журналистской этики. 2019. Т. 4. № 3. С. 85-12.

УДК 001.2; 004.81; 004.946

ВЛИЯНИЕ СЕТЕВЫХ МЕДИА НА ФОБИИ И УРОВЕНЬ ПСИХОЛОГИЧЕСКОЙ ТРЕВОЖНОСТИ В АСПЕКТЕ КОГНИТИВНОЙ БЕЗОПАСНОСТИ

Мельник Вероника Родионовна
Северо-Западный институт управления – филиал РАНХиГС
Средний просп. В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: melnik.roni@mail.ru

Аннотация. В статье анализируется проблема влияния провокативных публикаций в сетевых медиа на социальные фобии аудитории и опасность воздействия на ментальные структуры.

Ключевые слова: когнитивное поведение; фобии; информационная безопасность; психологическая тревожность; аудитория; медиа.

INFLUENCE OF NETWORK MEDIA ON PHOBIAS AND THE LEVEL OF PSYCHOLOGICAL ANXIETY IN THE ASPECT OF COGNITIVE SECURITY

Melnik Veronica
Northwestern Institute of Management - branch of RANEPA
57/43 Middle Av V.I., St. Petersburg, 199178, Russia
e-mail: melnik.roni@mail.ru

Abstract. The article analyzes the problem of the influence of provocative publications in online media on social phobias of the audience and the danger of influencing mental structures.

Keywords: cognitive behavior; phobias; information security; psychological anxiety; audience; media.

Критический обзор научной литературы показал, что коммуникативная агрессия вызывает человеческий страх и психологическое напряжение, тревоги, отчаяние, безысходность, а также может порождать ненависть, злобу. В психологической литературе исследуется в основном проблема типологии фобий и причины возникновения массовых паник [1, 2], делается акцент на том, что коммуникативные агрессии ведут к депрессиям, потере жизненных ориентиров и деморализации. Более того, трагические или резонансные события, происшествия и тревожные ситуации не только «обостряют устойчивые страхи и тревоги человека», а «вызывают активный отклик у пользователей социальных сетей».

Эмпирическую базу исследования составили публикации в электронных версиях газеты «Московский комсомолец», «Комсомольская правда», сетевого издания «Топор». Выбор сетевых изданий обусловлен их популярностью и ориентированностью в основном на моложеную аудиторию. Хронологические рамки исследования 25 ноября 2022 г. — 25 февраля 2023 г. В качестве метода исследования использовался контент-анализ (выборка сплошная), единицами анализа были отдельные тексты, содержащие потенциально социальные фобии, а единицами анализа стали заголовки с деструктивным содержанием, в которых отражались какие-либо патологии.

Результаты соотнесены с данными, полученными социологической организацией КРОС, ежеквартально измеряющей национальный индекс тревожности и составляющей рейтинг фобий россиян на основе анализа СМИ и социальных сетей и данными Страхового Дома ВСК и социологической фирмы НАФИ. Почти 30% россиян боятся инфляции и роста цен в 2023 г., падения доходов или тяжелой болезни (по 27 %), переживают за своих детей (25 %), новой пандемии (20 %) [3].

Результаты исследований показали, что молодежная аудитория активно реагирует на шок-контент. Провокативные публикации нередко вызывают спектр негативных эмоций, подвергая личность испытанию страхом.

В ходе исследования выяснилось, что провокативный дискурс предполагает предвзятые оценки событий, а под влиянием негативных факторов, прежде всего СМИ, люди становятся более подозрительными, настороженными и демонстрируют пренебрежение нормами морали.

В отношении 2023 г. года россияне допускают развитие негативных сценариев, в качестве угроз указывают: высокую инфляцию и рост цен, а также падение жизненного уровня (это связывают с СВО и западными санкциями); эскалацию конфликта с Западом (война с США и НАТО, возможность ядерного удара); диверсии (хлопки, пожары на предприятиях, повышенный уровень террористической угрозы); культуру отмены России и (проявления русофобии); финансовую нестабильностью и сокращение количества платежных инструментов (курс рубля, отключение Visa и MasterCard) [3]. При сопоставлении заголовочных комплексов выбранных изданий и результатов социологических опросов, показывающих индексы тревожности, можно обнаружить их связь. Показательны, например, броские заголовки материалов, опубликованных только в одном номере «Московского комсомольца» (25 февраля 2023): «Грянет буря: Путин переворачивает шахматную доску Украинского конфликта», 15 февраля 2023).

Повышают уровень тревожности публикации с так называемым шок-контентом. «Московский комсомолец» выходит с заголовками: «Ноги пропавшей модели нашли в холодильнике: подробности дикой истории»; Родители пострадавших школьников рассказали подробности о новосибирской банде «Ашановских)»; «Гончую застрелили на центральной улице в Подмосковье». Газета «Комсомольская правда (толстушка), освещает скандалы в среде шоу-звезд, выносит на первую полосу сенсационные заголовки: «Семью звезды Папиных дочек» разрушили алкоголь наркотики?»; «Пороховщикова сводил с ума и убивал собственный дом»; «Почему Костомарова довела до ампутация банальная пневмония»; «Макаревич торгует вином, а Моргенштерн нищает»; «Школьник поспорил, что соблазнит учительницу и...влюбился»; «Муж бил Гузееву гантелью по голове»; «Создатели фильма чуть моргалы друг другу не выкололи»; «Скорпинский маньяк собрался жениться»; «Что скрывают владельцы бассейна, где утонула дочка Конкина»; «Из снега на могиле Фриске делают приворотное зелье». «Сможет ли MakSim петь после возвращения с того света»; «Мужа расчлененной модели-красавицы арестовали при попытке скрыться».

На первую полосу, а не в раздел «Происшествия», попадают материалы о трагедиях, которым тем самым придается сенсационность: «Трагедия в Казани: почему дети убивают детей»; «Ельцина погубила тяга к власти и алкоголю».

Нарушая этические правила, «Комсомольская правда» сразу за речью президента РФ В. В. Путина, произнесенной накануне чтимого россиянами праздника «Дня защитника Отечества», дает подборку материалов, обесценивающих значимость официальной информации, с показательными заголовками: «Четвероногая кинозвезда не смогла переварить говяжье лакомство», «Младенец едва не умер во время обрезания», «Тренер

утонувшей синхронистки не замечала ее смерти шесть минут»; «Юный блогер пытался сделать эффектное селфи» (Московский Комсомолец № 33-2023 22/02/23).

В указанных изданиях, по нашим подсчетам, более 30% составляют публикации, в которых воспроизводятся какие-то патологии. Таким образом, актуальность темы определяется тем, что феномен страха мало изучен в теории массовой коммуникации. Это ставит перед научным сообществом необходимость разработки защитных механизмов от деструктивных информационных потоков, влияющих на поведенческие и когнитивные фобии. Крайне необходимо на уровне государства и гражданских структур прогнозировать последствия деструктивного воздействия на когнитивное и психологическое поведение людей.

СПИСОК ЛИТЕРАТУРЫ

1. Schneider S., Margraf J. Agoraphobie und Panikstörung. Hogrefe Verlag. Göttingen. Hogref, 2017.
2. Быков И. А., Гладченко И. А. Коммуникативная агрессия в России: анализ мнений будущих политологов и журналистов // Центрально-российский вестник социальных наук. 2018.Т. 13. № 1. С. 94–100.
3. Индекс тревожностей — спецпроект 2022 [Электронный ресурс]. URL: https://www.cros.ru/ru/exploration/research/3479/ (дата обращения 26.08.2023).
4. Россияне назвали главные страхи 2023 года [Электронный ресурс] // Ведомости. 22 декабря 2022. URL:https://www.vsk.ru/about/press_center/news/rossiyane_nazvali_glavnie_strahi_2023_goda/ (дата обращения 26.08.2023).

УДК 304.444

МЕДИЙНЫЕ РЕСУРСЫ В ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ АТАКАХ НА РОССИЙСКУЮ ГОСУДАРСТВЕННОСТЬ

Мельник Галина Сергеевна
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: menik.gs@gmail.com

Аннотация. Статья посвящена анализу психологических ресурсов оппозиционных российских сайтов, направленных на дискредитацию представителей органов власти и разрушение конституционных основ государства.

Ключевые слова: медиаресурсы; информационная безопасность; когнитивные технологии; психологические методы воздействия; информационная среда.

MEDIA RESOURCES IN INFORMATION AND PSYCHOLOGICAL ATTACKS ON RUSSIAN STATEHOOD

Melnik Galina
St. Petersburg State University,
7-9 University Emb, St. Petersburg, 199034, Russia
e-mail: menik.gs@gmail.com

Abstract. The article is devoted to the analysis of the psychological resources of oppositional Russian sites aimed at discrediting representatives of government bodies and destroying the constitutional.

Keywords: information security; cognitive technologies; psychological methods of influence; information environment.

В текстах сетевых медиа нередко организуются информационные атаки на объекты критической инфраструктуры, природную среду, информационную среду, органы государственного управления, государственных и общественных деятелей [1]. В связи с этим возникают проблемы обнаружения экстремистских источников и оперативного анализа общих данных, охватывающих три основных аспекта: «методы обнаружения, выполняющие идентификацию источника и проверку целостности носителей, загруженных в социальные сети, анализ происхождения платформ, позволяющий идентифицировать платформы для обмена, и алгоритмы проверки мультимедиа» [2]. Центр экспертиз СПбГУ, выполняющий такую работу по заказу прокуратуры, МВД, следственных органов создает научную базу для распознавания сценариев информационно-психологических атак и определения маркеров экстремистских медиатекстов. Рассмотрим типичные подходы оппозиционных сетевых медиа к работе с аудиторией.

Результаты исследования. На сетевых площадках организуются оппозиционные сообщества, формируются модели протестного поведения. Информационные ресурсы становятся центрами координации оппозиционных сил, которые ведут развернутую пропагандистскую работу, внедряя альтернативные символы (например, новый бело-сине-белый флаг РФ вместо триколора) и ценности. Из источников исходят призывы к свержению существующей власти. Смысловым ядром политических текстов становятся провокация и антагонизм [3]. «Ущербная антагонистическая модель политической коммуникации реализуется в агрессивной информационной среде, порождая жесткое противостояние, а использование политическими акторами манипулятивного потенциала дезориентирует аудиторию, делает беспомощной, погружает в пучину иррациональности» [4]. Атрибутами оппозиционного текста являются: «призыв к деятельности», «обоснование необходимости деятельности», «оправдание необходимости деятельности», «пропаганда негативного отношения к кому-либо (дискредитация)». Высказывания носят системный характер. Дискредитация представителей

органов власти достигается путем создания негативных образов президента России, правительственных структур Российской Федерации, чиновников. Типичным «образцом» подобных текстов является Манифест Легиона «Свобода России», Русского Добровольческого Корпуса и Национальной Республиканской Армии (размещен на платформе Telegram), где заявляется цель — «координация своих действий по вооружённому сопротивлению путинскому фашизму»). В подобных текстах обильно используются яркие определения, эпитеты («братоубийственная война», «путинская тирания», «опозоренный путинской властью триколор»), а также номинации и ярлыки («Путин — узурпатор власти», «Военный преступник, поправший Конституцию», «поджигатели войны», «грабители», «угнетатели народов России», «приспешники Путина» и «пособники узурпатора», «изменники Родины» и др.). Лейтмотивом звучит тема уничтожения. Называются объекты уничтожения. «Мы объявляем бизнесменов, зарабатывающих свои деньги на коррупции и связях с чиновниками — изменниками Родины и пособниками узурпатора. Имущество тех, кто не покается и не выступит публично против этой власти и ее войны, и они сами будут нами *уничтожаться*. Мы объявляем работников силовых структур пособниками узурпатора. Те, кто не сложит оружие и не снимет погоны — будут нами *уничтожаться», «*те, кто не сложит свои полномочия, будут нами *уничтожаться», «*кремлёвский режим должен быть *уничтожен* во имя мира на планете и сохранения жизней россиян и украинцев*»,* «Мы объявляем военные грузы и грузы тех, кто зарабатывает на войне и помогает ей финансово-законными целями, которые будут нами *уничтожаться*», «Имущество тех, кто не покается и не выступит публично против этой власти и ее войны, и они сами будут нами *уничтожаться»*.

В текстах называются насильственные способы действия, основной из которых — вооруженное сопротивление властям. Силовые действия направлены на свержение конституционного строя («Путин будет нами низложен и уничтожен»; «Только бескомпромиссные и решительные силовые действия могут остановить преступную банду Путина и его приспешников»). В документах прямо указано, что свержение власти будет осуществляться вооруженным (насильственным) путем: ««Легион «Свобода Росси»«, «Русский Добровольческий Корпус» и Национальная Республиканская Армия организуют координацию своих действий по вооружённому сопротивлению путинскому фашизму». Кроме того, есть утверждение, что оружие уже есть («взяли оружие в руки, чтобы бороться исключительно с узурпаторами власти в России, поджигателями и организаторами войны и их прислужниками и финансистами»). Заметим, что «Национальная республиканская армия/Роспартизан» (НРА) взяла на себя ответственность за организацию убийства 2 апреля 2023. военкора Владлена Татарского, до сих пор является открытым ресурсом.

Создатели публичного канала «Национальная Республиканская Армия/Роспартизан» используют когнитивные технологии, ориентируясь на прием идентификации. Местоимение «мы» используется ими при апелляции к разным целевым аудиториям: 1) *к солдатам*: Мы призываем солдат российской армии прекратить стрелять в наших братьев из других стран — Грузии, Сирии и других странах!»; 2) *ко всем россиянам:* «Мы призываем всех россиян вступать в наши ряды»; «Мы призываем жителей России следовать нашему примеру и оказывать все виды сопротивления преступному российскому режиму вплоть до его полного уничтожения; 3*) к сочувствующим*: «Где бы вы не были — боритесь как мы, боритесь вместе с нами, боритесь лучше нас!» 4) *к оппозиции* «Мы призываем представителей российской оппозиции и простых граждан отринуть все сомнения и разногласия и присоединиться к нашей борьбе».

Несмотря на контроль за информационными ресурсами со стороны Роскомнадзора, судебные решения в отношении деструктивных источников, разработку технологий выявления информационных атак в социальной сети, количество экстремистских сетевых ресурсов не уменьшается. Существование оппозиционных ресурсов по-прежнему представляет собой серьезную угрозу национальной безопасности страны, поскольку подрывает доверие у части населения к управляющим структурам, национальному политическому режиму.

СПИСОК ЛИТЕРАТУРЫ

1. Болмарт М. А. Государственное управление в сфере борьбы с терроризмом // Экономика и бизнес: цифровая трансформация и перспективны развития: Материалы междунар. науч.-практ. конференции, в 2-х тт. Т. 1. М.: Изд-во: АНО ВО «Ин-т бизнеса и дизайна», 2022. С. 20-27.
2. Cecilia Pasquini, Irene Amerini & Giulia Boato. Media forensics on social media platforms: a survey // EURASIP Journal on Information Security. 4 (2021) URL: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-021-00117-2
3. Володенков С.В. Интернет-технологии как инструмент воздействия на современные национальные политические режимы // Дискурс-Пи. Политические науки, 2017. С. 65-72.
4. Золоева З. Т., Койбаев Б.Г. Некоторые проблемы правового противодействия экстремистским проявлениям в информационно-телекоммуникационной сети Интернет // Гуманитарные и юридические исследования. 2018. № 4. С. 170ownload/3519/20-026-01.pdf. (дата обращения: 29.08.2023).

УДК 304.444

МАССМЕДИА ГЕРМАНИИ КАК СРЕДСТВО КОГНИТИВНОГО ИСКАЖЕНИЯ РЕАЛЬНОСТИ

Мисонжников Борис Яковлевич
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: b.misonzhnikov @spbu.ru

Аннотация. В условиях обостренного противостояния России и Запада противником применяются когнитивные механизмы ведения информационно-психологической войны. С целью насаждения в обществе выгодных западному политическому истеблишменту идей используются массмедиа, и можно наблюдать содержательную деградацию, которую переживают некогда авторитетные издания. Органом пропаганды стала и газета Frankfurter Allgemeine Zeitung (FAZ).

Ключевые слова: пропаганда; западные массмедиа; когнитивная война и когнитивная безопасность; газета Frankfurter Allgemeine Zeitung.

GERMAN MASS MEDIA AS A MEANS OF COGNITIVE DISTORTION OF REALITY

Misonzhnikov Boris
St. Petersburg State University,
7-9 University Emb, St. Petersburg, 199034, Russia
e-mail: b.misonzhnikov @spbu.ru

Abstract. In the conditions of an aggravated confrontation between Russia and the West, the enemy uses cognitive mechanisms of information and psychological warfare. In order to plant ideas beneficial to the Western political establishment in society, the mass media are used, and one can observe the substantial degradation that once authoritative publications are experiencing. The Frankfurter Allgemeine Zeitung (FAZ) newspaper also became a propaganda organ.

Keywords: propaganda; Western mass media; cognitive warfare and cognitive security; Frankfurter Allgemeine Zeitung newspaper.

Пропаганда как направленное идеологическое воздействие на аудиторию осуществляется при помощи текстовых поликодовых комплексов, в которых доминируют, как правило, вербальные системы. Методы и приемы текстового воздействия противостоящих, а зачастую и враждебных сил, возможно идентифицировать с помощью когнитивных наук, понимания сущности когнитивного моделирования. Дж. Лакофф отмечает: «В нашем стремлении понять мир мы используем когнитивные модели. В частности, мы используем их при теоретическом осмыслении мира, при создании научных теорий, равно как и теорий для повседневного употребления» [1]. Это позволяет нам идентифицировать семантику текстовых моделей в области лингвистической прагматики, т. е. аспектов отношений знаков и тех, кто их применяет. Тем самым устанавливается характер текстового влияния на формирование общественного мнения. Это влияние может осуществляться с благой целью оптимизации и регулирования социальных процессов, а может использоваться как средство манипулирования и управления людьми в корыстных и нередко разрушительных и преступных устремлениях. Через языковые практики, которые напрямую связаны с сознанием, через акты речевого общения с человеком можно воздействовать на его ментальные предпочтения, генерировать и корректировать соответствующие стимулы, провоцирующие не только отдельные поступки, но и детерминирующие стратегические модели поведения — поведенческие паттерны. А они в конечном счете формируют шаблоны поведенческих реакций, и человек может стать объектом манипулирования и совершить поступки в интересах чуждых, а то и враждебных сил.

Результаты исследования. Налицо факт систематического речевого — прежде всего дискурсного — воздействия на индивида, которое осуществляется западными массмедиа и носит крайне предвзятый и негативный характер. Это воздействие посредством дискурса — актуализированного связного текста, который соотносится с политическими, социокультурными, психоэстетическими и другими факторами современной действительности и реализуется, прежде всего, через систему массмедиа. Их усилиями искажается реальность, производится подмена гуманитарных приоритетов и духовных ценностей. Масштабы информационно-психологической войны, которая ведется против России, значительны. И. Ф. Кефели подчеркивает: «Средства и технологии информационно-психологической войны, действующие и в мирное время, способны нанести противнику не меньший ущерб, чем средства вооруженного нападения, а информационное оружие, построенное на базе технологий психологического воздействия, обладает значительно большей поражающей, проникающей и избирательной способностью» [2]. По этой причине важно обезопасить себя и общество от возможного негативного и разрушительного влияния идей, которые могут преднамеренно внедряться в когнитивные процессы и системы.

В последнее время можно наблюдать содержательные трансформации, которые переживают многие некогда солидные и авторитетные издания. Есть все основания констатировать: происходит стремительная деградация практически всех газетных «флагманов» западного мира, и они утрачивают право считаться качественными. Сохраняя формальные признаки принадлежности к некогда почетной типологической модели, эти газеты допускают неприемлемые методы профессиональной деятельности — прибегают к приемам содержательных подлогов и становятся соучастниками низкопробных пропагандистских акций. Об этом свидетельствуют и публикации изданий Германии. Остановимся на Frankfurter Allgemeine Zeitung (FAZ), которая в прошлом была консервативной и довольно авторитетной газетой. Ее предшественницу, Frankfurter Zeitung, даже Гитлер долго не мог закрыть и сделал это только после ареста Рихарда Зорге, который, работая в Японии, был корреспондентом газеты и на ее страницах во времена нацизма публиковал свои уникальные статьи.

Сегодня FAZ встроена в пропагандистскую систему Запада и использует самые вульгарные манипуляционные технологии, вследствие чего утрачивает уважение значительной части аудитории. К

сожалению, это отнюдь не частный случай. В свое время П. Бурдье говорил о том, что «„серьезные» журналисты и газеты понемногу теряют свой характер и вынуждены идти на уступки логике рынка и маркетинга» [3, 98]. Проще говоря, вынуждены бессовестно продаваться. Этим путем пошла и FAZ.

Еще до начала специальной военной операции на Украине редакция FAZ была уличена журналистом Ф. Шефером в использовании некорректной по отношению к России лексики: FAZ заявляла, что российское руководство в Сирии ведет «войну на уничтожение» (Vernichtungskrieg). Данная лексическая единица имеет резко негативную коннотацию и выполняет явную когнитивно-пропагандистскую функцию. Шефер обратил внимание на то, что это выражение, ставшее «стандартным словоупотреблением», совершенно не соответствует действительности и разрушает «немецкую культуру памяти». «Войну на уничтожение», по словам журналиста, вели нацисты против СССР, что привело к массовому уничтожению гражданского населения [4].

В последнее время, в условиях обострившегося противостояния России и Запада, язык вражды в FAZ приобрел беспрецедентный уровень ожесточения и агрессии. Правда, и раньше журналисты этой газеты, которая пыталась еще сохранять видимость объективности, время от времени позволяли себе глумливое отношение к политике российского государства. Это проявлялось, в частности, у некоторых авторов в трикстерстве, никак не отвечающем статусу газеты. Исследование данного стиля речевого поведения позволило прийти к следующему заключению: «Трикстерство в политической журналистике, которую считают качественной, явление, пожалуй, странное, но не совсем новое. Просто в разное время оно то ослабевало, то, оказываясь востребованным, актуализировалось — иной раз даже в вульгарных формах — особенно в периоды политического напряжения и отсутствия убедительных и бесспорных аргументов. Если нет полноценной доказательной базы, то это надо как-то компенсировать» [5]. Позже FAZ заняла откровенно русофобскую позицию и превратилась в орган проамериканской пропаганды. Авторы газеты прибегают даже к самым примитивным приемам дезинформации в стремлении внедрить в сознание читателей нужные идеи. Так, Ю. Альтвэгг, корреспондент FAZ и журналист с большим опытом, обвинил французскую журналистку А.-Л. Боннэль в том, что она выступила на стороне «путинской пропаганды», т. е. лишь за то, что она высказала свое мнение. Информация точная. Действительно, Боннэль поддержала российскую позицию. Но важно то, что Альтвэгг попутно утверждал: факта «сожжения людей в Одессе», мол, не удалось доказать [6]. И это при наличии множества документальных свидетельств, включая видеоматериалы! Утверждение высказано мимоходом, утвердительно и якобы не требует доказательств. Ассерторический смысл — конечно, искусно смоделированный — утверждению придает фактологическая точность предыдущего суждения. Ложь, таким образом, внедряется в систему когнитивных установок аудитории.

Деструктивная и, по сути, подрывающая основы морали, профессионального достоинства и объективности позиция FAZ даже на Западе стала вызывать резкую критику. Известный в Германии политик и публицист В. Хюбнер раскритиковал франкфуртскую газету в статье под заголовком — «FAZ — пропаганда войны и травля вместо серьезной журналистики» [7]. С явно риторическим вопросом обратился к читателям Ш. Франк: «Цензура и пропаганда в FAZ?» Статья с этим заголовком была опубликована в сетевом издании Die Achse des Guten и вызвала шквал читательских комментариев, крайне негативно, зачастую в оскорбительной и даже непристойной форме оценивающих позицию газеты: sybille eden — «FAZ и Völkischer Beobachter (официоз Третьего рейха. — Б. М.), пожалуйста, скажите, в чем теперь между ними разница???»; Michael Neus — «FAZ? Она у меня идет на растопку камина»; Armin Reichert — «Кто по своей воле читает FAZ, тот также полагает, что ХДС — это консервативная партия. От идиотов — для идиотов» и т.д. [8]. Всего было опубликовано более 80 осуждающих FAZ откликов.

Развивающиеся и имманентные индивиду когниции, процессы ментального текстового конструирования и воздействия, коррелируют с такими образованиями первостепенной важности, как представления, верования, убеждения, ценности, и обладают, будучи глубоко интегрированными в сознание индивида, значительным эффектом влияния. Именно они становятся целью западного политического истеблишмента, использующего массмедиа в своих интересах. В эту систему когнитивных диверсий оказались втянуты и почти все крупнейшие западные газеты, которые до недавнего времени считались качественными. Их профессиональный статус кардинально меняется, поскольку действительно качественные издания не могут быть органами политической пропаганды и игнорировать реальный ход событий.

СПИСОК ЛИТЕРАТУРЫ

1. Лакофф Д. Женщины, огонь и опасные вещи: что категории языка говорят нам о мышлении / пер. с англ. И. Б. Шатуновского. М.: Языки славянской культуры. 2004. 792 с.
2. Кефели И. Ф. Глобальные риски современного мира // Пролегомены когнитивной безопасности. Коллективная монография. СПб. : ИД Петрополис, 2023. 488 с.
3. Бурдье П. О телевидении и журналистике / пер. с фр. Т. В. Анисимовой, Ю. В. Марковой. М. : Прагматика культуры; Институт экспериментальной социологии, 2002. 160 с.
4. Schäfer V. Die Wiederkehr des «Untermenschen». Wie deutsche Medien über Russland im Syrienkrieg schreiben — und letztlich nur von Deutschland berichten. 2018. 27. März.
5. Мельник Г. С., Мисонжников Б. Я. Лингвистические приёмы антироссийской пропаганды — новый тренд массмедиа Германии // Гуманитарный вектор. 2020. Т. 15, № 5. С. 99–109.
6. Altwegg J. Heldin der russischen Wahrheit. Die französische Kriegsreporterin Anne-Laure Bonnel ist zur Paradezeugin von Putins Propaganda geworden. Ihr Film über den Donbass ist wie gemacht dafür // Frankfurter Allgemeine Zeitung. 2022.11. März.
7. Hübner W. FAZ — Kriegspropaganda und Hetze statt seriöser Journalismus // PI- NEWS (Politically Incorrect). 2022. 12. Apr . URL: https://www.pi-news.net/2022/04/faz-kriegspropaganda-und-hetze-statt-serioeser-journalismus/
8. Frank S. Zensur und Propaganda in der FAZ? [Электронный ресурс] // Die Achse des Guten. 2023. 23. Febr. URL: https://www.achgut.com/artikel/zensur_und_propaganda_in_der_faz (дата обращения: 20.06.2023).

УДК 001.2; 004.81; 004.946

К ВОПРОСУ О ПОНЯТИИ КОГНИТИВНОГО ПРОСТРАНСТВА

Плебанек Ольга Васильевна
Университет при Межпарламентской Ассамблее ЕврАзЭс
Смолячкова ул.,14/1, Санкт-Петербург, 194044, Россия
e-mail: plebanek@mail.ru

Аннотация: в статье предлагается обоснование места категории «когнитивное пространство» в теории безопасности. В силу того, что прогнозирование, анализ и предотвращение рисков и угроз существованию социума осуществляется в знаково-символической форме, а постановка адекватных целей деятельности зависит от выработки необходимых символических средств и единства понимания этих символов, в эпоху прокси-войн становится необходимым разработка модели когнитивного пространства.

Ключевые слова: артифицированная среда; знаково-символические средства; прокси-война; когнитивное пространство.

ON THE QUESTION OF THE CONCEPT OF COGNITIVE SPACE

Plebanek Olga
University at the Interparliamentary Assembly of EurAsEC
14/1 Smolyachkova St, St. Petersburg, 194044, Russia
email: plebanek@mail.ru

Abstract: the article offers a justification of the place of the category «cognitive space» in the theory of security. Due to the fact that forecasting, analysis and prevention of risks and threats to the existence of society is carried out in a symbolic form, and setting adequate goals of activity depends on the development of the necessary symbolic means and unity of understanding of these symbols, in the era of proxy wars it becomes necessary to develop a model of cognitive space.

Keywords: stratified environment; symbolic means; proxy war; cognitive space.

Основной закон существования живого — обеспечение безопасности организма, транслирующего свой генотип последующим поколениям. Критерием эволюционной успешности той или иной формы живого является способность вида к численному увеличению, занятию всех возможных экологических ниш и длительность существования во времени [1]. По мере усложнения биоты усложняются и средства обеспечения безопасности, эволюционируя от организмических средств — покровы, способность к движению и т.д. к способности прогнозирования, использованию внеорганизмических средств защиты, созданию искусственных объектов и построения эффективных коллективных стратегий выживания.

Человеческие популяции подчиняются тем же законам существования, как и все популяции живых существ: эволюционно успешные формы организации человеческих сообществ стремятся к численному увеличению, распространению на все пригодные для жизни и эксплуатации территории и максимальной трансляции своей жизненной модели во времени [2]. Человек отличается от других видов живых существ тем, что его видовая стратегии выживания является:

а) артифицированной (или техногенной) — защита от рискогенных природных и социальных агентов осуществляется посредством искусственных средств защиты, создание и использование которых требует взаимодействия;

б) коллективной — в силу самого длительного периода созревания взрослой особи осуществление защиты всегда является делом коллектива;

в) коммуникативной — в соответствии первыми двумя факторами, безопасность индивида находится в зависимости от совершенства коммуникативных средств;

г) знаково-символической — все предшествующие специфические для вида Homo Sapiens особенности обеспечения безопасности могут осуществляться только в знаково-символической среде, посредством которой формируются цели долгосрочной и краткосрочной деятельности, регулируются взаимодействия и проектируются технические объекты.

Вследствие того, что именно знаково-символические средства обеспечивают эффективность функционирования всей системы безопасности, на поздних стадиях развития техногенной среды решающее значение имеют когнитивные механизмы безопасности.

На стадии функционирования масштабных макрообщностей — цивилизаций, эффективность организационных структур (политико-правовых, производственных, этнокультурных и т.д.) все больше зависит от: а) согласованности когнитивных процессов, б) единства в понимании основных ценностей и смыслов и в) от адекватности выработанных абстрактных категорий и символов условиям в которых существует популяция и условиям, в которые предстоит обеспечивать безопасность.

Современная эпоха характеризуется глобальным противостоянием цивилизационных систем и переходом противоборства в фазу прокси-войн [3], в которых основная роль отводится когнитивно-психологическому воздействию. Когнитивно-психологическое воздействие на противника не только осуществляется на превентивном и преэмптивном этапе противоборства, но и зачастую заменяет другие формы войны. Когнитивно-психологическое воздействие становится возможным и осуществляется посредством разрушения когнитивного

пространства, в которых функционируют специфические для общественной системы смыслы, идеалы, формирующие цели и модели деятельности. Тема когнитивной безопасности поднята в коллективной монографии [4], однако, понятие когнитивного пространства обсуждается пока в контексте лингвистических проблем, а не в контексте теории безопасности.

Современная эпоха характеризуется также повышенной рискогенностью и летальностью технических и когнитивных средств (от деструктивных идеологий до средств нейролингвистического программирования), что ставит задачу формирования такого когнитивного пространства, в котором существовали бы единые для человечества смысложизненные ценности и единое понимание ценностных категорий.

Для осуществления этой задачи — формирование когнитивного пространства, в котором возможно осуществление коммуникации в общей знаково-символической системе, с общим представлением о наиболее важных константах бытия, необходима разработка модели когнитивного пространства.

В настоящее время проблема разграничения понятий когнитивного пространства и смежных с ним — картина мира, ментальное пространство, информационное пространство и т.д. (см. например, [5]) — уже ставится в научных исследованиях, однако пока не существует ни общепринятого определения этого понятия, ни даже предварительной модели когнитивного пространства. Вместе с тем, чтобы эффективно осуществлять противодействия когнитивным разрушительным воздействиям на общественную систему, разрабатывать систему психологической защиты необходимо опираться на понимание структуры когнитивного пространства, знание элементов из которого оно состоит и его принципиальные отличия от информационного пространства, которое может перекрывать границы социума, но не выполнять функции согласования позитивной деятельности социальных контрагентов.

В западных исследованиях термин когнитивного пространства известен с 70-х гг. XX в., но считается, что впервые осуществил попытку представить модель когнитивного пространства П. Певерелли в 2000 г., который выделил два элемента когнитивного пространства — социальный субстрат и когнитивный элемент сообщества (общие взгляды, символы, общий язык, общие фоновые знания о мироустройстве и т.д.) [6]. Однако, в отечественной психологической науке разрабатываемый на основе работ Л. Н. Леонтьева деятельностный подход [7], заставляет ввести в структуру когнитивного пространства еще один компонент — деятельность. Так как именно характер деятельности определяет когнитивность вовлеченных в нее (деятельность) субъектов, и именно деятельность детерминирует необходимость формирования новых смыслов и абстрактных символов, отражающих эти смыслы.

СПИСОК ЛИТЕРАТУРЫ

1. Шмальгаузен И. И. Проблемы дарвинизма. Изд. 2-е, переработанное и дополненное. Л. : Наука, 1969
2. Назаретян А. П. Антропология насилия и культура самоорганизации: Очерки по эволюционно-исторической психологии. Изд. стереотип. М.: ЛЕНАНД, 2017. 256 с.
3. Бартош А. А. Прокси-война. М. : Горячая линия Телеком, 2023. 256 с.
4. Пролегомены когнитивной безопасности. Коллективная монография / Под редакцией И. Ф. Кефели. СПб.: ИД «Петрополис», 2023. 488 с.
5. Егорова М. А. «Когнитивное пространство» и его соотношение с понятиями «ментальное пространство», «когнитивная база», «концептосфера», «картина мира» // Вестник ИГЛУ, 2012. С.61 -68
6. Гуревич Л. С. О правомерности использования термина «когнитивное пространство» в лингвистических исследованиях // Вестник Ч. : ЧитГУ, 2009. № 5 (56). С. 134-140
7. Леонтьев А. Н. Деятельность. Сознание. Личность. М., 1975. 304 с.

УДК 303.62; 316.7

ТЕОРИЯ ФРЕЙМИНГА И ПОЛИТИЗАЦИЯ СМИ (НА ПРИМЕРЕ ЗАМАЛЧИВАНИЯ ЗАПАДНЫМИ МЕДИА ПРОБЛЕМЫ СБРОСА ЯПОНИЕЙ ЯДЕРНЫХ ОТХОДОВ В МОРЕ)

Тань Лэи
Высшая школа журналистики и массовых коммуникаций
Санкт-Петербургского государственного университета
1-я линия В. О., 26, Санкт-Петербург, 199004, Россия
e-mail: tanleyiroyi@gmail.com

Аннотация: 24 августа 2023 г. на первой атомной электростанции Фукусимы в Японии начался процесс сброса радиоактивных отходов в море, который завершился 11 сентября. В течение этого периода западные средства массовой информации практически не освещали данное событие, демонстрируя коллективное молчание. Некоторые из медиа искажали факты, перекладывая ответственность за сброс на Китай. Когда видеоблогеры пытались опросить граждан западных стран, большинство респондентов оказались не в курсе событий, а некоторые даже подверглись дезинформации со стороны СМИ. В данной статье с использованием теории фрейминга будет проведен анализ и размышление на тему политизации медиа в контексте молчания западных СМИ после сброса ядерных отходов в море Японией. Рассматриваются три аспекта: содержание массмедийных сообщений, общественное мнение и политические решения.

Ключевые слова: ядерные отходы; западные СМИ; международное общественное мнение; теория фрейминга; китайско-американские отношения.

RAMING THEORY AND POLITICIZATION OF THE MEDIA (ON THE EXAMPLE OF WESTERN MEDIA SILENCING THE PROBLEM OF JAPAN DUMPING NUCLEAR WASTE INTO THE SEA)

Tan Leyi
School of Journalism and Mass Communications, Saint Petersburg State University
26 1st Line, V. I., St. Petersburg, 199004, Russia
e-mail: tanleyiroyi@gmail.com

Abstract. On August 24, 2023, the process of discharging radioactive waste into the sea commenced at Japan's Fukushima Daiichi Nuclear Power Station, concluding on September 11. During this period, Western media outlets largely ignored the event, displaying collective silence. Some even distorted the facts, shifting the responsibility for the waste discharge onto China. When video bloggers attempted to interview citizens from Western countries, the majority were uninformed about the event, and some were even misled due to inaccurate journalism. This paper employs framing theory to analyze and reflect on the politicization of media in the context of Western media's silence following Japan's disposal of nuclear waste into the sea. It examines three aspects: the content of mass media messages, public opinion, and political decisions.

Keywords: nuclear waste; western media; international public opinion; framing theory; Sino-American relations.

13 апреля 2021 г. японский кабинет министров официально принял решение о сбросе радиоактивных отходов с первой атомной электростанции Фукусимы в Тихий океан. Это решение немедленно вызвало острое внимание и протесты прибрежных стран. На сегодняшний день, несмотря на противодействие международного сообщества, Япония односторонне продолжает сброс, транспортируя радиоактивные отходы по трубопроводу на расстояние 1500 км от себя и в районе Северного экватора.

Первая партия сброса, составляющая около 7800 тонн, была завершена с 24 августа по 11 сентября 2023 г. Китай, возможно, станет первой страной, пострадавшей от этого сброса. Действия Японии нарушают обязательства по «Конвенции ООН по морскому праву». Япония до сих пор не смогла доказать безопасность такого сброса. Данные, опубликованные самой Японией, показывают, что почти 70% обработанных радиоактивных отходов все еще не соответствуют стандартам. Сброс в море не является единственным возможным вариантом утилизации радиоактивных отходов и тем более не является самым безопасным и оптимальным методом. Япония, мотивированная экономическими соображениями, выбирает морской сброс, перекладывая риски ядерного загрязнения на всё человечество и серьезно угрожая праву на здоровье граждан разных стран [1].

Теория фрейминга в области массовых коммуникаций впервые заимствована из психологии. Американский антрополог Грегори Бейтсон (Gregory Bateson) впервые предложил концепцию «фрейма» в 1955 году в работе «Теория игр и фантазий», определив фрейм как «ограниченный контекст». Позднее американский социолог Эрвинг Гофман (Erving Goffman) систематизировал теорию фрейминга и применил её к исследованиям в области культурной социологии.

С тех пор теория фрейминга официально вошла в исследовательскую область журналистики и массовых коммуникаций, становясь объектом изучения в этой дисциплине. В контексте журналистики и массовых коммуникаций, фрейминг означает структуру понимания и интерпретации новостного события, формируемую медийными организациями через выборочное редактирование, распространение или удаление фактов, характеристик, деталей и вытекающих из них последствий. Внутри данного фрейма определенные аспекты новостного события акцентируются, в то время как информация, считаемая медиа нерелевантной или нежелательной для акцентирования, фильтруется. Это приводит к формированию различных рамок отчетности [2].

С точки зрения содержания массмедиа и новостных отчетов, как источника информации для аудитории, уменьшение объема отчетности, искажение фактов или даже незначительные коррекции могут оказать значительное влияние на общественное мнение и социальную ситуацию. После того как Япония начала сбрасывать ядерные отходы в море, соседние страны, такие как Китай, Северная Корея, Южная Корея и Россия, выразили решительный протест против этого крайне безответственного действия со стороны японского правительства. Однако западные СМИ, которые ранее так озабочены были выбросами углекислого газа из Китая, внезапно умолкли.

Главные страницы крупных западных медиасайтов почти не освещали этот вопрос. Многие блогеры, находящиеся за границей и проводящие уличные опросы на тему сброса ядерных отходов Японией, часто получали ответы вроде «Читал новости, но не видел ничего по этому вопросу» или «Слышал, что это недобросовестный поступок Китая», в то время как лишь немногие знали факты.

С точки зрения общественного мнения, у аудитории также есть свои когнитивные рамки для понимания, которые играют неоспоримую роль в восприятии медийной информации. То есть теория фрейминга не только фокусируется на том, как средства массовой информации конструируют себя, но и на том, какой эффект текст оказывает на аудиторию. Люди слишком сильно зависят от информации, полученной через устоявшиеся медиаплатформы, что создает чувство доверия.

Все данные, опубликованные на этих платформах, могут быть приняты аудиторией на веру, не проводя дополнительной проверки, что влияет на их восприятие событий. Это также означает, что в политических

событиях можно полностью полагаться на мощный распространительный потенциал медиаплатформ для контроля общественного мнения и влияния на результат. В отношении инцидента с сбросом отходов в Фукусиме, заголовок статьи в «Forbes» гласит: «Почему разумно, что Япония сбрасывает ядерные отходы Фукусимы в океан», тем самым квалифицируя это как разумное действие. Вводная часть статьи ясно квалифицирует этот инцидент: «Это именно то, что они должны сделать». Однако вопрос о том, является ли это действие разумным, не должен решаться американцами, а должен оцениваться пострадавшими из Китая, Кореи и других прибрежных регионов.

С точки зрения политического принятия решений, изменение медийных рамок напрямую зависит от национальных интересов, и политизация медиа сильно влияет на роль средств массовой информации в политике. Например, в первом десятилетии нового века, китайско-американские экономические отношения продолжали быстро развиваться, входя в относительно стабильный период.

Западные СМИ в это время часто использовали рамки «прогресса и развития» для освещения Китая. В 2010 г., когда Китай стал второй по величине экономикой мира, отношения между Китаем и США пережили переломный момент. Администрация Обамы в этом же году начала стратегию «ребалансировки в Азиатско-Тихоокеанском регионе». С точки зрения США, Китай перешел из статуса потенциальной угрозы в реальное и крупнейшее препятствие, что привело к резкому увеличению негативного и критического освещения в отношении Китая.

В моральных рамках репортажей «The New York Times» и «The Washington Post» о спорах в Южно-Китайском море, Китай представлен как агрессор и нарушитель безопасности, в то время как США идеализированы как стражи порядка и защитники малых стран [3].

Исследования и критические анализы теории фрейминга весьма обширны как внутри страны, так и за рубежом, и все сходятся во мнении, что в медиапроизводстве не существует информации, которая не была бы оформлена в определенные рамки. Западные СМИ постоянно создают новостные рамки, которые соответствуют западной идеологии и интересам, с целью контроля международного общественного мнения и препятствия развитию Китая. Особенно с развитием новых медиа, представленных интернетом, политизация медиа стала нормой современной политической жизни.

Современный политический процесс подвергается огромным изменениям под влиянием массовых медиа, и использование медиа для достижения политических целей стало новой формой современной политической жизни.

Долгое время, по мере роста международного статуса Китая, основные СМИ развитых западных стран стремятся захватить лидирующие позиции в международном дискурсе по вопросам, касающимся Китая, создавая тем самым негативный образ страны на мировой арене. Это не только сильно влияет на отношение других стран к Китаю, но и делает медиа инструментом политической борьбы. Это также демонстрирует важную роль политизации медиа и СМИ в политике.

Процесс производства новостей со стороны журналиста носит селективный характер. Установка медиафрейма связана с салиентностью новости и приданием «заметности» тому или иному вопросу [4]. Как производители новостного контента, массовые средства информации должны всегда оставаться на страже объективности и честности; читатели, в свою очередь, должны обладать способностью к критическому мышлению и поиску истины; участники международного общественного мнения должны правильно оценить баланс сил на международной арене, четко понимать текущую обстановку и различать «друзей» и «врагов» [5].

На данный момент некоторые китайские медиа уже могут говорить напрямую на зарубежных платформах, рассказывая» китайскую историю» в соответствии с собственной концептуальной рамкой. Это уже огромный прогресс.

Для завоевания международного дискурса необходимо, чтобы «китайская версия китайской истории» получала признание и осознание на мировой арене, что постепенно изменит образ Китая в глазах западных СМИ.

В общем, медиатизация политики стала новой формой современной политической жизни. Понимание её смысла, особенностей и влияния поможет освоить базовые закономерности медиатизированной политики, способствуя тем самым прогрессу современной демократии и обеспечению стабильности и развития политического общества. Кроме того, анализ стратегии рамочного оформления новостей поможет прояснить цели западных СМИ в отношении Китая. Это облегчит прогнозирование и реагирование Китая на международные вопросы и направления общественного мнения, предоставляя интеллектуальную поддержку для изменения существующего доминирования западных СМИ в международном дискурсе.

СПИСОК ЛИТЕРАТУРЫ

1. Чэнь Б. Японские ядерные сточные воды в море, насколько велико воздействие? // New People's Weekly. 2023. № 24. С. 56-59.
2. Kang J. Как американские мейнстримные СМИ корректируют рамки освещения Китая — на примере The Wall Street Journal // Media. 2016. № 20. С. 45-47.
3. Xin Bin. Анализ фреймов в сообщениях китайских и американских СМИ о споре вокруг Южно-Китайского моря // Journal of Foreign Languages. 2018. № 03. С. 20-26.
4. Кушнерук С. Л. Стратегическое фреймирование как объект зарубежной коммуникативистики: истоки, проблемы, перспективы // Коммуникативные исследования. 2022. Т. 9, № 2. С. 243-259.
5. Чжун Вэй. Исследование коллективного молчания западных СМИ в связи с инцидентом с ядерными сточными водами с точки зрения теории фрейминга // Journalism Research Guide № 05. С. 55-57.

УДК 070

МЕДИАПОТРЕБЛЕНИЕ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: НЕГАТИВНЫЕ И ПОЗИТИВНЫЕ ПОСЛЕДСТВИЯ

Тюнина Екатерина Владимировна
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: e.v.tiunina@gmail.com

Аннотация. Анализируются особенности процесса и ключевые характеристики медиапотребления. Описываются тенденции медиапотребления в 2023 году.

Ключевые слова: аудитория; СМИ; медиапотребление; контент; медиатизация, негативные последствия, информационная безопасность.

MEDIA CONSUMPTION: PROCESSES, CHARACTERISTICS, TRENDS

Tiunina Ekaterina
Saint Petersburg State University
Universitetskaya Emb, 7-9, St. Petersburg, 199034, Russia
e-mail: e.v.tiunina@gmail.com

Abstract. The author analyzes the features of the process and key characteristics of media consumption, describes the trends in media consumption in 2023.

Keywords: audience; media; media consumption; content; mediatization; negative consequences; information Security.

Цифровизация позволяет создавать информационные ресурсы, новые оригинальные форматы вовлечения людей в социальные практики, значительно влияя на качество медиапотребления в современном мире. Медиапотребление — это использование медиапродукции, при котором потребитель удовлетворяет свои информационные, коммуникационные, экономические и другие потребности и интересы и которое является неотъемлемым фактором современной медиакультуры [1]. Объектом медиапотребления выступает медийный продукт, а средствами — технические устройства, с помощью которых медийный продукт распространяется среди аудитории. Исследователи выделяют несколько основных особенностей процесса медиапотребления в современной жизни:

Рутинизация, то есть потребление медиапродукции на регулярной основе и с задействованием разных каналов информации — как традиционных, так и новых (телевидения, радио, печатной прессы, книг, Интернета и других). При этом вовлеченность аудитории в медийное пространство неуклонно растет, доступ к Интернету становится одной из главных жизненных потребностей.

Активность, под которой подразумевают прикладывание определенных усилий для пользования каналами информации (например, поиск в Интернете новостей на интересующую тему).

Ситуативность — способность и возможность применять разные источники информации (скажем, в салоне автомобиля прослушивание радио или аудиокниги, дома просмотр новостной ленты в Интернете).

Техническая оснащенность — для получения информации необходим посредник в виде технического устройства (телевизора, компьютера, смартфона и пр.).

Квалифицированность — набор навыков, необходимых для получения и информации [2].

В научном дискурсе регулярно отслеживаются тенденции медиапотребления. Так, в 2023 г. исследователи выделили следующие тенденции:

Увеличение времени, которое средний пользователь ежедневно тратит на цифровые медиа. Если в 2020 г. этот показатель составлял 474 минуты (это 7 часов 54 минуты, или треть жизни), то в 2023 г. эксперты спрогнозировали его рост до 500 минут в день.

Отмирание печатного медиаканала. Эпоха газет и журналов, которые давно переживают кризис, завершается: согласно одному из маркетинговых исследований, только 26% потребителей рассматривают возможность обращения к этому ресурсу для поиска информации о покупках. У поколения Z (родившихся с 1996 г. по 2012 г.) доля еще ниже — 19 %.

Рост роли смартфонов в медиапотреблении. В 2023 г. на смартфоны приходится 35% всего потребления медиа, причем большая его часть приходится на приложения.

Использование мобильных телефонов для социального взаимодействия. В 2023 году число пользователей социальных сетей в мире достигло 4,89 миллиарда.

Снижение терпимости к рекламе. В 2022 г. 66 % респондентов пропускали рекламу или платили за ее блокировку. И их число постоянно увеличивается [3].

Американский исследователь Брайан Макфадден обозначил четыре ключевые характеристики: 1) Все медиа обеспечивают либо информационную, либо развлекательную потребность, либо обе сразу. В любом случае потребителю медиа важна скорость, с которой он может получить информацию или эмоцию; 2) Решение о потреблении медиа в определенный момент времени не зависит от цены, если доступ к источнику медиа

является бесплатным или право на потребление медиа (например, по подписке) уже получено. Хотя это не относится к медиа с оплатой за просмотр, фактор нулевых или необратимых затрат влияет на большинство типов медиа; 3) Потребители медиа выбирают из нескольких медиаисточников. СМИ всегда соревнуются за внимание отдельных потребителей, но не всегда составляют друг другу конкуренцию в плане контента; 4) Если позволяет медиаплатформа, информацию будут потреблять постепенно и в разное время [4].

В последние годы были разработаны новые научные антропологические теории, которые оказали глубокое влияние на изучение медиапотребления. Данные исследования помогают понять, как медиа работают в различных социальных и культурных контекстах, влияют на повседневную жизнь. Одной из наиболее влиятельных теорий в антропологии медиапотребления является медиатизация. Согласно теории медиатизации, медиа проникают во все сферы нашей жизни и формируют социальную реальность; не просто передают информацию, а создают новые формы социального взаимодействия; влияют на понимание индивидом себя и окружающего мира.

По мнению М. Кастельса, сетевое общество имеет ряд, как позитивных, так и негативных последствий для общества, включая изменения характера работы, власти, культуры и идентичности:

– В сетевом обществе все больше людей работают в неформальном секторе экономики, а не в формальном секторе экономики.

– Власть в сетевом обществе распределена по многим различным узлам сети, а не сосредоточена в руках небольшого числа людей или организаций.

– Культура в сетевом обществе становится более разнообразной и космополитичной.

Люди в сетевом обществе могут формировать свои идентичности на основе различных факторов, таких как их интересы, навыки и ценности, а не только на основе их пола, расы или национальности [5].

Медиа могут использоваться для изменения общества. Они могут, с оной стороны, распространять новые идеи и ценности, способствовать формированию новых социальных движений, а, с другой стороны служат, деструктивным фактором разрушения традиционных отношений, ценностей и моральных принципов. Томпсон утверждает, что медиа являются мощным инструментом, который может использоваться как для добра, так и для зла. По его мнению, важно осознавать влияние медиа на общество и использовать их ответственно [6].

Исследователь Н. Кудлери констатирует, что цифровые медиа не просто изменили способы производства и потребления медиа, но и привели к трансформации общества и культуры; сделали возможным более интерактивное и вовлекающее общение, способствовали формированию новых социальных сетей и сообществ; расширили возможности для самовыражения и самопрезентации; дали возможность индивидам создавать собственный медиаконтент и делиться им с другими, что позволило им формировать свои собственные идентичности [7].

При этом, отмечает исследователь, цифровые медиа имеют ряд негативных последствий: могут быть использованы для распространения дезинформации и пропаганды, создания зависимости и изоляции, что создает угрозу информационной безопасности общества и личности. Потому, уверен он, важно осознавать эти последствия, чтобы использовать цифровые медиа ответственно.

СПИСОК ЛИТЕРАТУРЫ

1. Крайникова Т. С. Медиапотребление : обзор рецепций явления // Вестник Воронежского государственного университета. Серия Филология. Журналистика. В., 2013. № 2. С.167-170.
2. Мурзина Е. В. Медиапотребление в условиях трансформации современного общества // Вестник Сургут. Го.педагогического ун-та 2020. № 5 (68). С. 229–230.
3. 5 big media consumption trends for 2023 [электронный ресурс] // Cure Media. URL: https://www.curemedia.com/media-consumption-trends/ (дата обращения: 26.07.2023).
4. McFadden B. A Theory of Media Consumption and Demand, with Implications for Media Industry Structure and Firm Strategy (April 23, 2019) [Электронный ресурс]. URL: https://ssrn.com/abstract=3097558 (дата обращения 26.07.2023).
5. Manuel Castells. The Rise of the Network Society (2010) [Электронный ресурс]. URL https://onlinelibrary.wiley.com/doi/epdf/10.1002/9781444319514.fmatter (дата обращения 26.07.2023).
6. John B. Thompson. The Media and Modernity (1995) [электронный ресурс]. URL https://www.sup.org/books/extra/?id=2348&isbn=0804726795&gvp=1 (дата обращения 26.07.2023).
7. Nick Couldry. Media, Society, World: Social Theory and Digital Media Practice (2012). С.22-29.

УДК 316.6

ИССЛЕДОВАНИЕ ПОВЕДЕНИЯ И ПСИХОЛОГИИ ВЕРБАЛЬНОГО НАСИЛИЯ СРЕДИ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ-СМИ

Чжоу Шэннань
Высшая школа журналистики и массовых коммуникаций СПбГУ
1-я линия В.О., 26, Санкт-Петербург, 199034, Россия
e-mail: st097863@student.spbu.ru

Аннотация. Новые медиаплатформы создали людям удобную среду для общения во времени и пространстве и предоставили возможность для выражения различных идей и эмоций. Тем самым расширилось поле и для чрезмерного выражения негативных эмоций и бессмысленного вербального насилия. В этом тексте исследуется поведение и психология аудитории, подвергающейся насилию в СМИ.

Ключевые слова: новые медиа, вербальное насилие, поведение аудитории, психология аудитории.

ANALYSIS OF BEHAVIOR AND PSYCHOLOGY OF VERBAL VIOLENCE AMONG INTERNET MEDIA USERS

Zhou Shengnan
Higher School of Journalism and Mass Communications St. Petersburg State University
1st line V.O., 26, St. Petersburg, 199178, Russia
e-mail: st097863@student.spbu.ru

Abstract. New media platforms have created a convenient environment for people to communicate across time and space and have provided an opportunity to express various ideas and emotions. This has expanded the scope for excessive expression of negative emotions and senseless verbal violence. This text explores the behavior and psychology of audiences exposed to media violence.

Keywords: new media; verbal violence; audience behavior; audience psychology.

Пользователей, вовлеченных в повсеместное насилие в интернет-медиа, можно разделить на участников (субъект), жертв (объект) и сторонних наблюдателей. Интернет-группы различного масштаба занимаются дискриминацией и оскорблением других, исходя из разных мотивов: кто-то из желания «выплеснуть» негативные эмоции, кто-то из любопытства, кто-то ради справедливости, кто-то ради личной выгоды, а кто-то из-за непреднамеренного распространения информации. Большинство пользователей Сети имеют сразу несколько мотивов и участвуют в вербальном насилии, основанном на множестве причин.

Интернет объединяет мир в целом, а недорогая бесконтактная связь позволяет получать «весьма экономически эффективные» результаты. Однако это также делает онлайн-контент вульгарным, порой жестоким и оскорбительным, и оставляет много неопределенности в информационном содержании. Некоторые пользователи, руководствуясь простой справедливостью и моральными нормами, надеются использовать давление общественного мнения для исправления поведения, отклоняющегося от социального порядка.

Потребители информации узнают о происшествиях через интернет-СМИ и участвуют в распространении свежих сплетен и новостей. Хотя такого рода поведение осуществляется в форме онлайн-насилия, оно призвано способствовать социальной справедливости и осуждать людей с отклонениями от моральных норм. Однако некоторые выражают злобные эмоции. Вербальное насилие, преследующее такого рода цели, обычно начинается с онлайн-атак в целях мести со стороны некоторых пользователей сети, что также относится к киберзапугиванию, иными словами, «кибербуллингу» (Cyberbullying) [1].

Гюстав Лебон писал в книге «Психология народов и масс», что «группа» – это люди, которые собираются вместе при определенных условиях» [2], и группа участников медианасилия всегда будет образовывать кластер людей со схожими мышлением или психологией. Если чьи-то высказывания, острые темы и т. д. стимулируют нервное возбуждение эмоциональных групп с определенными общими познаниями и идеями, то члены этих групп временно собираются вместе, чтобы совместно бросать вызовы и выражать свое недовольство группам или отдельным лицам, которые с ними не согласны. Если эти социальные группы с одинаковой установкой проявят подавляющую силу, а их желания окажутся значительно сильнее, чем у других групп, эта группа будет думать, что ее собственные взгляды имеют превосходство в поле общественного мнения. Они уверуют в то, что обладают высшей юрисдикцией и статусом над «ущербным» меньшинством людей. Такое поведение «расширения собственных возможностей» невидимо позволяет группе с большим количеством последователей иметь «временную верховную власть» над общественным мнением, то есть представляют собой онлайн-насилие [3].

Тем не менее, качество пользователей сети различается, а решения, принимаемые их группами, не всегда справедливы и рациональны. Кроме того, некоторые пользователи со своей индивидуальностью сталкиваются с угрозой «информационной наготы» в «состоянии цифрового выживания», что внушает им страх. Поэтому, чтобы соответствовать интересам группы, интегрироваться в «коллектив» и не стать новой мишенью онлайн-насилия, некоторые люди с индивидуальными личностями будут вынуждены «поддаться» голосу группы. Это непреднамеренно усиливает высокомерие онлайн-злоумышленников.

В 1974 г. Элизабет Ноэль-Нойман предложила концепцию «спирали молчания», в которой кратко изложено это правило: когда люди выражают свои мысли и мнения и видят то, с чем они согласны, если их точка зрения широко приветствуется, то люди подсознательно, считают, что их точка зрения «популярна», «правильна и разумна»; наоборот, в случае, если люди не видят точку зрения, с которой они согласны, или даже видят ее, но не имеют поддержки большинства людей или подвергаются критике со стороны многих – люди предпочтут хранить молчание и не выражать свое мнение [4]. Зрители, вовлеченные в онлайн-насилие, подвержены этим влиянием. Они не будут предпринимать существенных действий, но их внимание к инциденту непреднамеренно увеличит популярность инцидента. Другими словами, хотя зрители не высказываются и не занимают определенную позицию, они также станут косвенными сторонниками, вызывая у всех в обществе иллюзию, что использование «киберзапугивания» для решения проблем «разумно и справедливо».

Язык интернет-медиа является производным от современного социального взаимодействия, а слова в медианасилии обычно эмоциональны и оскорбительны. Хотя развитие технологий значительно улучшило права каждого человека на доступ к СМИ, личная власть часто ограничена. Когда происходит массовая атака на медиа-платформы, стороны, подвергающиеся насилию, обычно, оказавшись в водовороте общественного мнения, оказываются в слабом положении. В знаменитом ток-шоу «Джимми Киммел в прямом эфире» однажды был

прочитан отрывок под названием «Когда знаменитости читают порочные твиты». Известная актриса кино и телевидения Кристен Белл подверглась критике со стороны пользователей сети за «некрасивость» и не могла сдержать слез; поп-певица Кеша подверглась насилию со стороны назойливо ее осаждающих из-за дела об изнасиловании, которое так и не было разрешено... Кроме того, некоторые пользователи сети применяли в своих выступлениях слова, которые хорошо известны публике или которые люди могут сразу понять. Таким образом, уникальный язык сетевых атак сформировался и используется повсеместно.

Американский профессиональный рестлер Джон Сина однажды сказал на китайском языке в видеоролике, снятом для продвижения фильма «Форсаж 9»: «Доброе утро, Китай, теперь у меня есть мороженое (Бинчилин), я очень люблю мороженое (Бинчилин), но «Форсаж 9» лучше, чем мороженое (Бинчилин)». Некоторые злобные пользователи сети сочли это лестью Китаю и осудили Джона Сину. С тех пор «Бинчилин» также считается оскорбительным расистским сленгом и символом этнической дискриминации в Китае.

Очевидно, что аудитория виртуального онлайн-пространства не всегда представляют собой здравомыслящих людей. Под защитой анонимности некоторые пользователи могут смело выражать свое мнение, это также порождает некоторые безответственные слова и поступки. Некоторые высказывания, сделанные по поводу кибернасилия, являются неподтвержденными онлайн-инцидентами и крайне предвзяты. Однако они могут нанести большой вред карьере, жизни и душе заинтересованных сторон, а также вызвать ряд неблагоприятных последствий для сторон, включая беспокойство и депрессию, злоупотребление наркотиками, проблемы со сном, отягощение существующих заболеваний и даже приводят к убийству или самоубийству [5]. В то же время общественные ресурсы были незаконно присвоены, сетевая экология потеряла порядок, а общественные пространства утратили право голоса, препятствуя обмену взглядами и выражению мнений теми, кто действительно в этом нуждается. Если не препятствовать этой ситуации в течение длительного времени, признание обществом онлайн-насилия неизбежно возрастет, а доверие к СМИ будет падать, вызывая более масштабные социальные противоречия и конфликты.

Поэтому, как члены нового столетия, пользователи Интернета должны усилить моральную самодисциплину и повысить свою осведомленность о защите конфиденциальности; лидеры общественного мнения должны укрепить собственное чувство социальной ответственности и сгладить общественные настроения; официальные медиаплатформы должны усилить контроль; а правительство должно строго формулировать соответствующие законы и правила и другие меры. Только таким образом можно будет создать позитивную медиасреду и улучшить эмоциональный фон каждого отдельного пользователя.

СПИСОК ЛИТЕРАТУРЫ

1. Belsey, B. What is cyberbullying? 2004 [Электронный ресурс]. URL: http://www.cyberbullying.ca (дата обращения: 06.09.2023)
2. Гюстав Лебон. Психология народов и масс. – М.: Академический проект, 2011. – 238 с.
3. Юэ Цзяннин. Исследование феномена онлайн-насилия в контексте новых медиа // Руководство по исследованию новостей. 2020. № 3. С.94–96.
4. Сазонова А.А. Средства массовой информации как инструмент воздействия гуманитарных технологий на общественное сознание // Манускрипт. 2018. № 87(201). С.78–92.
5. Sheryl Puterman. What is the impact of online shaming and cyberbullying? 2020 [Электронный ресурс]. URL: https://www.jpost.com/jpost-tech/what-is-the-impact-of-online-shaming-and-cyberbullying-635134 (дата обращения: 07.09.2023).

УДК 004.81; 612.82

НЕЙРОНАУКИ – ОСНОВА ИССЛЕДОВАНИЯ ОСОБЕННОСТЕЙ ГОЛОВНОГО МОЗГА И МОДЕЛИРОВАНИЯ РАЗЛИЧНЫХ КОГНИТИВНО-ПОВЕДЕНЧЕСКИХ ПРОЦЕССОВ

Шангин Андрей Борисович
ФГБОУ ВО «Российский государственный педагогический университет им. А.И. Герцена»
наб. р.Мойки, 48, Санкт-Петербург, 191186, Россия
e-mail: andrej-shangin@yandex.ru

Аннотация. Рассматриваются научно-исторические аспекты формирования и развития нейронауки и различных её направлений в структуре изучения восприятия и переработки информации человеком, а также формирования различных паттернов поведения в структуре когнитивного воздействия различной направленности в современных условиях.

Ключевые слова: нейронаука, головной мозг, нейрон, рефлекторная дуга, информационное воздействие, нейросети, поведенческие паттерны.

NEUROSCIENCE IS THE BASIS FOR THE STUDY OF BRAIN FEATURES AND MODELING OF VARIOUS COGNITIVE–BEHAVIORAL PROCESSES

Shangin Anlrey
The Herzen Russian State Pedagogical University, 48 Moika nab., St. Petersburg, 191186, Russia
e-mail: andrej-shangin@yandex.ru

Abstrat. The scientific and historical aspects of the formation and development of neroscience and its various directions in the structure of the study of human perception and processing of information, as well as the formation of various patterns of behavior in the structure of cognitive impact of various directions in modern conditions are considered.

Keywords: neuroscience, brain, neuron, reflex arc, informational impact, neural networks, behavioral patterns.

Впервые термин «нейронаука» был использован в 1962 году в «Программе нейронаучных исследований» Массачусетского технологического института (США), которую возглавил профессор этого заведения Фрэнсис О. Шмитт [4]. Тогда же нейронаука была официально признана академической дисциплиной. Ряд отечественных учёных внесли значительный вклад в создание основ нейронауки. Знаменитый русский физиолог Иван Михайлович Сеченов, в своём труде «Рефлексы головного мозга» (1863 г.) впервые убедительно доказал, что «все акты сознательной и бессознательной жизни по способу происхождения суть рефлексы». Нобелевский лауреат Иван Петрович Павлов исследованиями в области условных (второсигнальных) рефлексов, расширил горизонты знаний в физиологии нервной системы. Николай Евгеньевич Введенский (1852-1922) открыл ритмический характер протекания нервного возбуждения. Алексей Алексеевич Ухтомский (1875-1942) создал учение о доминанте, как о форме взаимодействия между процессами возбуждения и торможения в центральной нервной системе, при которой господствующий (доминантный) очаг возбуждения не только тормозит протекание других рефлексов, но и одновременно усиливается за счёт других раздражений, захватывая, при длительном существовании всё новые и новые области головного мозга. Владимир Михайлович Бехтерев (1857-1927) – разработал различные методы терапии психических расстройств с помощью гипноза, активно изучал методы коллективного воздействия на массовое сознание [3]. Среди основных направлений нейронауки на современном этапе непосредственное отношение к анализу проблем обеспечения информационно-психологической и когнитивной безопасности имеют:

– когнитивная нейронаука, которая изучает взаимосвязи функций головного мозга с поведением и когнитивными процессами;

– вычислительная нейробиология, исследующая математические закономерности биологических аспектов функционирования нервной системы и поведения человека;

– нейропсихология – изучает мозговую организацию высших психических функций и их взаимосвязь с поведением;

– нейроинженерия – изучает возможности восстановления или замены элементов нервной системы;

– нейролингвистика – изучает нейронную основу лингвистических процессов;

– нейроэвристика – изучает процессы в структурах головного мозга с точки зрения взаимовлияния генетических факторов и социальной среды.

– нейросоциология – это научное направление междисциплинарного и многоуровневого характера, предметом изучения которого является взаимосвязи нейробиологических процессов в организме с особенностями различных социальных явлений и процессов на микроуровне (социальное взаимодействие в микросоциумах, личное принятие решений и пр.) при обязательным переносом этого подхода на макроуровень (различные социальные институты, социально-экономическую сферу, коллективными социальные нормы и др.). Содержание нейронауки определяются решением трех главных задач:

– насколько независимы друг от друга мозг и психика или же их нужно рассматривать как единое целое;

– насколько независимы группы нейронов в контексте своей «специализации» и могут ли они работать, как единое целое, все вместе;

– является ли сознание исключительно продуктом деятельности мозга и можно ли объяснить работу сознания только работой нейронов.

Нейронаука, сформировалась как один из разделов нейрофизиологии, занимаясь изучением нейронных процессов, анализом структуры нервной системы, процессами обработки информации в нервной ткани и механизмами, определяющими поведение животных и человека. Научный или критичный подход к изучению действительности и различных процессов, подразумевает наличие особого, аналитического склада ума, развитого логического мышления и сформированного собственного мнения на различные аспекты жизни. Совершенно очевидно, что наличие подобной привычки всё оценивать сквозь критические «фильтры» мозга, позволяет лучше противостоять влиянию информационного шума, негативной информации, постоянно передаваемой в различных СМИ и Интернете. И, в особенности, - подобный склад ума позволяет вполне успешно противостоять различным специальным влияниям в структуре когнитивной войны.

Правильно организованный мозг человека – это непробиваемый для врагов щит. Однако, он не формируется сам собой. Для этого необходима разнообразная, научно обоснованная, системная и последовательная подготовка населения, его отдельных групп (под различные задачи), которая будет давать возможность создавать тот самый «щит» когнитивной устойчивости перед агрессивными информационными воздействиями различного характера и направленности.

Также необходимо ответить на вопрос: почему постоянно эффективными оказываются самые «примитивные» с точки зрения восприятия информационные посылы, используемые во все века в структуре агитации, пропаганды и/или подрывной идеологической деятельности? Ответ на этот неочевидный вопрос находится в области нейронаук – нейробиологии, нейропсихологии и нейросоциологии одновременно, поскольку человек един в строении организма и взаимодействии его систем.

Главное – это энергетические особенности деятельности мозговых структур (нервных клеток и нейронных сетей) – мозг – очень энергоёмкая субстанция, поэтому, чем проще для его «восприятия» и «понятнее» информационное послание, содержание которого знакомо человеку - информация уже содержится в памяти – мозговых базах данных человека (оно уже знакомо), тем вероятнее что мозг (и человек вместе с ним) обратит внимание именно на него. Если это информационное воздействие достаточно длительное и постоянное, то

срабатывает эффект «знакомости» (вчера было то же самое) – облегчения восприятия в постоянно формирующейся нейронной сети. Кроме этого, постоянно действует механизм перевода информации из оперативной памяти в долговременную. В этом заключается важность структурированной и целенаправленной пропаганды/информационного воздействия с использованием слов – как уже было сказано, мозг «любит» воспринимать «простое» и «понятное» [1] .

Поскольку человек отличается от животного наличием морфологических субстратов в головном мозгу (центры Вернике и Брока), позволяющим воспринимать и воспроизводить речь (наряду с особым строением гортани) – развитой второсигнальной системы формирования условных рефлексов на основе словесной информации передаваемой посредством слов, то значимость этих слов приравнивается ко всем прочим источникам информации вместе взятым. Человек слышит некие слова, в которых заложен некий информационный посыл, призыв к действию или иное мнение. Что там заложено? Кем заложено? Для какой цели это сделано? В какой ситуации это сообщение приходит и про какие события – прошлые, текущие или будущие, говорит? Масса вопросов, масса вариантов ответа и, соответственно, - огромное количество вариантов воздействия на того, кто воспринимает.

Таким образом, ограничение (или исключение) ненужной (для одной группы) информации для масс, при одновременном регулярном использовании простых и эмоционально насыщенных информационных посылов для этих же масс, и дают тот самый эффект, обеспечивающий победу в когнитивной войне в стане противника.

СПИСОК ЛИТЕРАТУРЫ

1. Анохин К. Когнитом: на пути к единой когнитивной теории / Петербургский семинар по когнитивным исследованиям: доклады и стенограммы / под ред. Т. В. Черниговской, Т. Е. Петровой. – СПб.: Изд-во С.-Петерб. ун-та, 2022. – Т. 1: 2012–2015. – 272 с. С. 127-149.
2. Баарс Б., Гейдж Н. Мозг, познание, разум: введение в когнитивные нейронауки: в 2 ч. Ч.1 / пер.с англ. Проф. В.В. Шульговского. – М.: Лаборатория знаний, 2016. – 541 с.
3. Бехтерев В. М. Коллективная рефлексология. – Петроград: Колос. – 1921. – С. 39.
4. F. O. Schmitt, J. L. Oncley, R. C. Williams, M. D. Rosenberg, and R. H. Bolt. Biophysical Science: A Study Program. New York: Wiley and Sons, 1959.

УДК 327.8

ОСНОВНЫЕ НАПРАВЛЕНИЯ ИНФОРМАЦИОННОГО-ПОДРЫВНОЙ ДЕЯТЕЛЬНОСТИ ЗАПАДА ПРОТИВ РОССИЦЙСКОЙ ФЕДЕРАЦИИ: ПОЛИТОЛОГИЧЕСКИЙ АНАЛИЗ

Шевцов Владимир Сергеевич
Российский государственный гуманитарный университет
Каширское ш., 4, корп. 2, Домодедово, 142000, Россия
e-mail: speziell@mail.ru

Аннотация. В тезисах доклада автором раскрыта сущность и содержания информационно-подрывной деятельности. Представлены направления её осуществления странами Запада в отношении России. Сделаны выводы относительно системности подобной работы.

Ключевые слова: информационно-подрывная деятельность; информационно-подрывные действия, акции и кампании.

MAIN DIRECTIONS OF INFORMATION AND DISRUPTIVE ACTIVITIES OF THE WEST AGAINST THE RUSSIAN FEDERATION: POLITICAL ANALYSIS

Shevtsov Vladimir
Russian State University for the Humanities
4/2 Kashirskoe hw, bld 2, Domodedovo, 142000, Russia
e-mails: speziell@mail.ru

Abstract. In the abstract of the report, the author reveals the essence and content of information and subversive activities. The directions of its implementation by Western countries in relation to Russia are presented. Conclusions are drawn regarding the systematic nature of such work.

Keywords: information and subversion; information and subversive actions, actions and campaigns.

Информационно-подрывную деятельность с политологических позиций можно опередить как некую совокупность имеющих широкий спектр открытых, а также скрытых информационных мер (действий, акций, кампаний), которые объединены общим замыслом (сведены воедино) и осуществляются скоординировано в интересах достижения масштабной (наиболее значимой) геополитической цели. Средства оказываемого на Российскую Федерацию информационно-подрывного воздействия достаточно вариативны, их выделяют исходя из структуры самого информационного противоборства: информационно-психологические, информационно-технические, и, собственно, информационно-технологические (субкомпонент последних).

Отметим, что в соответствии с решаемой задачей применяются в том числе и политические технологии, и специализированные аппаратно-программные средства воздействия как на информационно-технические системы, так и на сознание целевых аудиторий (классов общества, профессиональных сообществ, групп по интересам, др.) Справедливо относят к средствам неправительственные и некоммерческие организации, а также фонды, используемые для подготовки и финансирования специальных действий, наносящих ущерб интересам России. Информационно-подрывная деятельность является основной формой организации информационного

противоборства, подготовка которой требует применения достаточно широкого набора инструментов, и что в современных условиях в контексте внешней политики позволяет считать её ключевым средством достижения конкретной политической (геополитической) цели Запада.

Реализуемая информационно-подрывная деятельность включает в себя как отдельно проводимые акты, так и включенные в состав более крупного стратегического замысла (например, информационной кампании). Исходя из понимания общей сущности информационно-подрывной деятельности, проводимой сегодня США, их сателлитами, можно уверенно констатировать, что сегодня она приобрела геополитический масштаб. Средства и инструменты её реализации выходят за рамки информационной сферы и направлены на создание условий, при которых руководство Российской Федерации подчинится политической воле Запада (в частности — США) и откажется от проведения самостоятельной и национально-ориентированной внешней политики.

Широкий спектр изученных научных источников, концептуальных / доктринальных документов стран Запада, политических установок и заявлений американского, европейского истеблишмента, комментариев официальный представителей профильных структур и комиссий, функционирующих в пределах российской юрисдикции, дают основания полагать, что направления информационно-подрывных действий, осуществляемых Западом в отношении российского государства, можно дифференцировать по направлениям:

1. Подрыв укрепляемой российской властью политической и социальной стабильности посредством создания в нашей стране условий, при которых будет нанесен ущерб государственной безопасности как на системном (общенациональном) уровне, так и на уровне подсистем (сфер жизнедеятельности общества и государства).

В рамках первого можно выделить следующие субнаправления:

- информационно-подрывные действия, преследующие целью нарушить политическую и социальную стабильность в Российской Федерации посредством дестабилизации обстановки в так называемых городах–центрах власти (наиболее крупных городах). Напомним, что наиболее опасные для государства протестные акции в период 2011–2013 гг. и 2017–2019 гг. проходили преимущественно в Москве, в меньшей степени — в Санкт-Петербурге. Из истории: августовский путч (кризис) 1991 г. и октябрьский путч 1993 г. также затронули преимущественно столицу России. Следует особо отметить, что Европа в сформулированных резолюциях еще с 2011 г. активно демонстрировала проамериканский курс и не дружественность своей политики: «Депутаты Европарламента приветствуют демонстрации в России как выражение стремления российского народа к большей демократии и осуждают подавление полицией мирных демонстраций…» [1]. В последующем были и иные акции подрыва авторитета государственной власти с использованием сомнительной доказательной базы. Кроме того, завершая свою посольскую деятельность в России Дж. Хантсман в канун парламентских выборов в России сообщил, что что будущее России не определено и в ближайшие годы ее «ожидают довольно интересные события» [2].

– информационно-подрывные действия, направленные на дестабилизацию политической обстановки на приграничных территориях. В этой связи напомним действия по восстановлению конституционного порядка в Чечне 1994–1996 гг. и контртеррористическую операцию на Северном Кавказе в период с 1999 по 2009 гг. Из более поздних событий это протесты в Ингушетии по причине переноса административных границ 2018–2019 гг. Все указанные обстоятельства объединяет устойчивое понимание того, что инспирировали их при активном участии европейских и американских спецслужб. В 2022–2023 г. зазвучали реваншистские лозунги грузинской оппозиции, призывавшей на фоне «бездействия» России в Нагорном Карабахе инициировать активные действия по возврату утраченных территорий [3]. С новой силой набирает обороты концепт государственного департамента США по реинкарнации концепции «Большой Кавказ» с центром в Тбилиси [4], в состав которого по его плану должны войти и прилегающие российские территории. Опасность складывающейся ситуации заключается в том, что Запад работает в ключе поиска уязвимостей регионов, позволяющих активизировать в них центробежные силы.

2. Сохранение и при возможности расширение сферы мирового влияния США посредством укрепления геополитического потенциала НАТО в ущерб интересам объединений (блоков, организаций), в которых состоит Россия. В рамках этого направления отметим системные действия США по позиционированию и продвижению ложных представлений о России, как угрозе «всему цивилизованному миру». Попутно в глобальном масштабе Западом решаются вопросы монополизации рынка вооружения и выключения из конкурентного процесса Рособоронэкспорта, обвиняемого в нарушении закона США о нераспространении оружия в отношении Ирана, Сирии и Северной Кореи [5]. В нынешних условиях еще более актуальной задачей Запада становится недопущение упрочения союза России и КНР, ведь это сопряжено с расширением Шанхайской организации сотрудничества, которую США рассматривают как инструмент сдерживания НАТО [6]. Параллельно ведется подрывная работа и против других структур, чрезвычайно важных с позиции безопасности России, особенно Организации договора о коллективной безопасности и т.д.

3. Установление контроля над ключевыми водными акваториями, особенно расположенными вблизи границ России, под предлогом расширения зон свободного судоходства. В рамках его реализации усилия Запада фокусируются на трех информационно-подрывных субнаправлениях:

– пересмотр Конвенции Монтрё, [7] которая не позволяет им на регулярной основе и без ограничений (класс судна, тоннаж и время пребывания) проходить Черноморские проливы и, тем самым, вводить значительные силы военно-морского флота в прилегающие к России водные акватории;

– лоббирование и поиск путей перевода Северного морского пути под международный контроль, чтобы обеспечить свое военное присутствие у северных границ России, ограничить возможности в области совместных инфраструктурных проектов России и КНР;

– создать очаг напряженности на Дальнем Востоке, где симбиоз политики США и Японии подогревает стремление последней быть более требовательной к «возврату» утраченных территорий, включая сценарии по их силовому захвату. Для этого уже сегодня при активном участии американской стороны создаются программы перевооружения и развития флота Японии. Формальный повод — военная активность КНР и КНДР [8].

Таким образом, с политологических позиций информационно-подрывная деятельность США и их союзников является достаточно системной, активной и пролонгированной во временном отношении. В рамках неё решаются с виду решаются исключительно локальные задачи, однако если их анализировать с системных позиций, то становится понятно, что осуществляются они в контексте общего стратегического замысла и что многие из них являются компонентами достаточно масштабной геополитической компании, сопоставимой с войной, по масштабному сдерживанию России.

СПИСОК ЛИТЕРАТУРЫ

1. Европарламент призвал Россию провести новые выборы в Госдуму. [Электронный ресурс]. URL: https://www.vedomosti.ru/politics/articles/2011/12/14 (дата обращения: 21.09.2023).
2. Запад раскрывает карты. [Электронный ресурс]. URL: https://planet-today.ru/geopolitika/item/112411 (дата обращения: 21.09.2023).
3. Грузинская оппозиция призвала вернуть Абхазию и Южную Осетию силовым путем. [Электронный ресурс]. URL: https://vz.ru/news/2023/9/26/1232126.html (дата обращения: 21.09.2023).
4. Грузия планирует стать центром Кавказа? [Электронный ресурс]. URL: https://vestikavkaza.ru/news/Gruziya-planiruet-stat-tsentrom-Kavkaza.html (дата обращения: 21.09.2023).
5. Imposition of Nonproliferation Measures Against Foreign Persons, Including a Ban on U.S. Government Procurement. URL: https://s3.amazonaws.com/public-inspection.federalregister.gov (дата обращения: 21.09.2023).
6. ШОС пугает США. [Электронный ресурс]. URL: https://russian.rt.com/opinion/1049816 (дата обращения: 21.09.2023).
7. Конвенция о режиме проливов (Конвенция о режиме Черноморских проливов) (Монтре, 20 июля 1936 г.). [Электронный ресурс]. URL:https://base.garant.ru/2541161 (дата обращения: 21.09.2023).
8. Япония готовит превентивные удары по КНДР, Китаю и РФ [Электронный ресурс]. URL: https://www.ng.ru/world/2022-11-22 (дата обращения: 21.09.2023).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ

УДК 004.8

СПОСОБ УСКОРЕНИЯ ПРОВЕДЕНИЯ ГЛОБАЛЬНОГО АПОСТЕРИОРНОГО ВЫВОДА С ИСПОЛЬЗОВАНИЕМ ТРЕТИЧНОЙ СТРУКТУРЫ

Абрамов Максим Викторович, Вяткин Артём Андреевич
СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: aav@dscs.pro, mva@dscs.pro

Аннотация. Данная работа определяет два фактора, за счет которых проведение глобального апостериорного вывода в алгебраической байесовской сети проходит быстрее с использованием третичной структуры, чем с использованием вторичной. Помимо этого указан способ, позволяющий с учётом выявленных факторов еще больше ускорить проведение вывода, использующего третичную структуру.

Ключевые слова: алгебраические байесовские сети; вероятностные графические модели; фрагмент знаний; третичная структура; вторичная структура; глобальный апостериорный вывод; машинное обучение.

A WAY TO SPEED UP GLOBAL POSTERIOR INFERENCE USING TERTIARY STRUCTURE

Abramov Maxim, Vyatkin Artyom
SPIIRAS – SPCRAS
39 14th line, V. I., St. Petersburg, 199178, Russia
e-mails: aav@dscs.pro, mva@dscs.pro

Abstract. This paper identifies two factors that make global posterior inference in an algebraic Bayesian network faster using a tertiary structure than using a secondary structure. In addition, a method is presented that takes into account the identified factors to further speed up the inference using the tertiary structure.

Keywords: algebraic Bayesian networks; probabilistic graphical models; knowledge pattern; machine learning.

Алгебраические байесовские сети являются подклассом вероятностных графических моделей, находящих свое применение в различных практических сферах, таких как, например, отслеживание визуальных объектов [1], создание цифровых двойников пользователей [2], анализ прочности материалов [3]. В теории алгебраических байесовских сетей одной из крупных задач стоит задача проведения глобального апостериорного вывода, который заключается в распространении влияния свидетельства, определяющего новую информацию. На текущий момент описаны два метода проведения глобального апостериорного вывода, использующие третичную и вторичную структуры алгебраической байесовской сети.

Ранее было показано [4], что при использовании третичной структуры проведение глобального апостериорного вывода проходит быстрее в 1.15–2 раза, чем при использовании вторичной структуры. Данная же работа будет направлена на выявление способа еще большего ускорения проведения глобального апостериорного вывода, использующего третичную структуру, за счет выявления факторов разницы во времени работы алгоритмов, описанных в статье [4].

Способ ускорения. Первым фактором, ускоряющим проведение глобального апостериорного вывода, является, несомненно, необходимость построения вторичной структуры, которое использует третичную структуру.

Однако были проведены вычислительные эксперименты по сравнению времени работы различных частей алгоритмов, которые показали, что существенную роль в ускорении играет другой фактор. Этот фактор заключается в использовании меньших по мощности свидетельств, распространяемых при проведении вывода.

В случае третичной структуры свидетельства формируются не большей мощности, чем при проведении вывода с использованием вторичной структуры, что достигается за счет использования нагрузок, находящихся все ближе к вершине-пустой нагрузке третичной структуры. При этом время распространения свидетельств в конкретные фрагменты знаний зависит экспоненциально от количества атомов в пропагируемых свидетельствах, отсюда и вытекает более быстрая работа алгоритма, использующего третичную структуру.

На основе данного наблюдения предлагается еще большее ускорение проведения глобального апостериорного вывода, использующего третичную структуру. В его алгоритме [5] на шаге 1 нагрузка выбирается произвольно, однако выбор меньшей по мощности нагрузки даст более быстрое время распространения свидетельства по вышеописанным выводам.

В данной работе были описаны факторы, которые дают более быстрое время работы алгоритма глобального апостериорного вывода, использующего третичную структуру алгебраической байесовской сети по сравнению со вторичной структурой, а также, на этой основе, определен способ ещё большего ускорения проведения вывода с использованием третичной структуры. Дальнейшие исследования могут быть направлены на выявление причин появления выбросов при проведении экспериментов в работе [3], что также способно определить пути для улучшения алгоритмов.

Работа выполнена в рамках проекта по государственному заданию СПБ ФИЦ РАН СПИИРАН № FFZF-2022-0003.

СПИСОК ЛИТЕРАТУРЫ

1. Ebert-Uphoff I., Deng Y. Causal discovery for climate research using graphical models // Journal of Climate. 2012. vol. 25. P. 5648–5665.
2. Kapteyn M. G., Pretorius J. V., Willcox K. E. A probabilistic graphical model foundation for enabling predictive digital twins at scale // Nature Computational Science. 2021. Vol. 1, No 5. P. 337–347.
3. Petrolo M., Carrera E. On the use of neural networks to evaluate performances of shell models for composites // Advanced Modeling and Simulation in Engineering Sciences. 2020. Vol. 7. P. 1–28.
4. Vyatkin A. A., Tulupyev A. L. Statistical Comparison of the Running Times of Global Posteriori Inference Algorithms in Algebraic Bayesian Networks // 2023 XXVI International Conference on Soft Computing and Measurements (SCM), Saint Petersburg, Russian Federation. 2023. P. 24-28, doi:10.1109/SCM58628.2023.10159044.
5. Вяткин А. А., Абрамов М. В., Харитонов Н. А., Тулупьев А. Л. Применение третичной структуры алгебраической байесовской сети в задаче апостериорного вывода // Вестник ЮУрГУ. Серия: Вычислительная математика и информатика. 2023. Т. 12, № 1. С. 61–88.

УДК 004.7.056.53

ВЛИЯНИЕ СОЦИОИНЖЕНЕРНЫХ АТАК НА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И ФУНКЦИОНИРОВАНИЕ РЕГИОНАЛЬНЫХ ГОСУДАСРТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Азаров Артур Александрович, Демидов Михаил Олегович, Савельев Павел Сергеевич
Северо-Западный институт управления – филиал РАНХиГС
Россия, Санкт-Петербург, Средний пр. В.о 57/43
e-mail: artur-azarov@yandex.ru

Аннотация: В статье описано влияние социоинженерных атак на развитие подходов в обеспечении безопасности и дальнейшего защищенного функционирования региональных государственных информационных систем. Представлены общие модели функционирования региональных государственных информационных систем. Описаны возможные уязвимости системы и представлены стратегии по минимизации социоинженерных атак на них.

Ключевые слова: социоинженерные атаки, государственные информационные системы, политики доступа.

INFLUENCE OF SOCIAL ENGINEERING ATTACKS ON SECURITY AND OPERATION OF REGIONAL GOVERNMENT INFORMATION SYSTEMS

Artur Azarov, Mikhail Demidov, Pavel Savelev
Northwestern Institute of Management - branch of RANEPA
57/43 Sredniy pr., St. Petersburg, 199178, Russia
e-mail: artur-azarov@yandex.ru

Abstract: The article describes the impact of social engineering attacks on the development of approaches to ensuring security and further secure functioning of regional government information systems. General models of the functioning of regional state information systems are presented. Possible system vulnerabilities are described and strategies for minimizing social engineering attacks on them are presented.

Keywords: social engineering attacks, government information systems, access policies.

Развитие современных региональных государственных информационных систем напрямую связано с этапом цифровизации различных функций органов государственной власти. В свою очередь, в процессе цифровизации и создания новых информационных систем особую актуальность приобретает вопрос обеспечения безопасности функционирования данных систем и хранения данных. В контексте данного исследования, мы рассмотрим различные зарубежные подходы к анализу защищенности пользователей региональных информационных систем.

Защита информации от социоинженерных атак является важным и актуальным направлением исследований в области информационной безопасности. Анализ защищенности информационной системы от социоинженерных атак в комплексе с программно-аппаратными методами защиты позволяет в значительной степени минимизировать вероятность успеха атаки злоумышленника [1].

В зарубежной практике для решения анализа защищенности пользователей региональных информационных систем используются следующие подходы:

- рассмотрение социотехнических атак на пользователей;
- решение исключительно инсайдерских атак на информационные системы;

– изучение представлений пользователей об информационной безопасности и взаимосвязи этих представлений с индивидуальными особенностями пользователей;

– анализ необходимости обучения пользователей основам информационной безопасности.

В настоящее время эти подходы как никогда актуальны для Российской Федерации, так как повышение давления зарубежных информационных центров на региональные государственные информационные системы может привести к нарушению конфиденциальности, переводу денежных средств пользователей на зарубежные счета, тиражированию персональной и служебной информации.

В связи с этим важнейшим вопросом для органов государственной власти, должно стать обеспечение безопасности существующих и разрабатываемых государственных информационных систем (в том числе регионального уровня). Используемые нами подходы и проводимые на их основе исследования в области защиты пользователей от социоинженерных атак помогут в создании многоуровневых систем безопасности региональных государственных информационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. А. А. Азаров, Т. В. Тулупьева, А. В. Суворова [и др.]. Социоинженерные атаки: проблемы анализа / – Санкт-Петербург: Санкт-Петербургская издательско-книготорговая фирма "Наука", 2016. – 349 с. – ISBN 978-5-02-039592-3. – EDN.XXPKVV.
2. Suleimanov A., Abramov M., Tulupyev A. Modelling of the social engineering attacks based on social graph of employees communications analysis // 2018 IEEE Industrial Cyber-Physical Systems (ICPS), 801–805 (2018).
3. Kharitonov N., Maximov A., Tulupyev A. Algebraic Bayesian Networks: The Use of Parallel Computing While Maintaining Various Degrees of Consistency // Studies in Systems, Decision and Control (199), 696–704 (2019).

УДК 004.7.056.53

СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ ФАКТОРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ФУНКЦИОНИРОВАНИЯ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В КОНТЕКСТЕ СОЦИОИНЖЕНЕРНЫХ АТАК

Азаров Артур Александрович, Демидов Михаил Олегович, Савельев Павел Сергеевич
Северо-Западный институт управления РАНХиГС
Россия, Санкт-Петербург, Средний проспект В.О., д. 57/43
e-mail: artur-azarov@yandex.ru

Аннотация: В докладе представлены результаты исследования, посвящённого анализу и обобщению существующих социально-психологических факторов обеспечения безопасности и функционирование государственных информационных систем. Выделяются намеренные и ненамеренные действия пользователей, которые могут привести к нарушению безопасности информации. К факторам, влияющим успешность социоинженерной атаки можно отнести большую численность штата организации, доступность информации о сотрудниках и поверхностное знакомство сотрудников с правилами информационной безопасности.

Ключевые слова: социоинженерные атаки, государственные информационные системы

SOCIO-PSYCHOLOGICAL FACTORS OF ENSURING THE SECURITY AND FUNCTIONING OF STATE INFORMATION SYSTEMS IN THE CONTEXT OF SOCIO-ENGINEERING ATTACKS

Artur Azarov, Mikhail Demidov, Pavel Savelev
North-West institute of management RANEPA
57/43 Sredny prospect VO, St. Petersburg, russia
e-mail: artur-azarov@yandex.ru

Abstract: The report presents the results of a study devoted to the analysis and generalization of existing socio-psychological factors in ensuring security and the functioning of government information systems. Intentional and unintentional actions of users that can lead to a violation of information security are identified. Factors influencing the success of a social engineering attack include the large number of staff in an organization, the availability of information about employees, and employees' superficial familiarity with information security rules.

Keywords: social engineering attacks, literature review, government information systems

Цифровизация – общемировой тренд, проявляющийся на уровне государственного управления во внедрении различных информационных систем в процессы принятия и реализации управленческих решений. Так в деятельности органов государственной власти Санкт-Петербурга используется порядка 106 государственных информационных систем [1], в работе которые используются персональные данные и финансовая информация. От их функционирования зависит эффективность реализации государственных функций и качество жизни горожан.

В настоящий момент изменение геополитической конъюнктуры и ухудшение международных отношений актуализировали вопросы защиты информации и разработки более совершенных методов защиты данных. Несмотря на существующие методы защиты, из фокуса внимания специалистов по информационной безопасности выпадают пользователи, обеспечивающие работу подобных государственных информационных систем. При должном воздействии на них извне, могут происходить утечки информации [2] или изменения в

функционировании информационных систем. Такие воздействия можно объединить термином социоинженерные атаки.

Настоящая работа посвящена анализу и обобщению существующих социально-психологических факторов обеспечения безопасности и функционирование государственных информационных систем.

Среди данных факторов можно выделить намеренные и ненамеренные действия пользователей, которые могут привести к нарушению безопасности информации [3]. Намеренные действия связаны с наличием мотивов направленных на удовлетворение собственных потребностей, основой ненамеренных действий является обработка пользователями различных почтовых вложений и телефонных обращений. К факторам, повышающим успешность социоинженерной атаки, можно отнести большую численность штата организации, использующей государственную информационную систему, доступность информации о сотрудниках, а также поверхностное ознакомление сотрудников с правилами информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Реестр государственных информационных систем Санкт-Петербурга (URL: https://reestr-gis.gov.spb.ru/gis)
2. Kotenko I., Chechulin A., Branitskiy A. Generation of Source Data for Experiments with Network Attack Detection Software // Journal of Physics: Conference Series (820), 12–33 (2017).
3. Социально-психологические факторы, влияющие на степень уязвимости пользователей автоматизированных информационных систем с точки зрения социоинженерных атак / Т. В. Тулупьева, А. Л. Тулупьев, А. Е. Пащенко [и др.] // Труды СПИИРАН. – 2010. – № 1(12). – С. 200-214.

УДК 629.12, 65.011, 681.518

ЦИФРОВОЕ РАБСТВО КАК УГРОЗА ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЛИЧНОСТИ ОТ ПРАВОВЫХ ИНСАЙДЕРОВ

Алексеев Анатолий Владимирович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., д. 3, Санкт-Петербург, 194064, Россия
e-mail: iapbgks@bk.ru

Аннотация. Поднимается проблема и обсуждаются факторы, угрозы и пути нейтрализации злоупотреблений организационно-информационного характера в современном электронном документообороте (ЭДО), обусловленные критическим проявлением негативных свойств человеческого фактора операторов ЭДО при выполнении ими должностных обязанностей и злоупотреблений служебным положении, в том числе при искусственном формировании недобросовестными юридическими лицами разного рода якобы «должников» (соответствующих информационных инцидентов) по оплате ЖКУ, особенно, в части ПЭС, нарушителей ПДД, информационного подавления разного рода «жалобщиков» за счет использования «технологий» массовой рассылки электронных писем «по клише», массового использования виртуальных информаторов и автоответчиков, подавления информационно-избыточными (без предметного рассмотрения) и многостраничными безответственными письмами. Сделан вывод, что подобную «цифровую бюрократию» следует рассматривать как критическую угрозу развития цифровой трансформации общества, ЭДО, которые в условиях цифровой доступности, массирования потоков ЭДО и юридических регламентов типа «исполнения в течение 5 дней после размещения сообщения в банке данных» создает для «информационно обнаженных» рядовых граждан обстановку «цифрового рабства». Предложено в развитие ФЗ-152 создать систему юридически значимой системы информационной безопасности личности от «правовых инсайдеров», в том числе из среды общества и государства.

Ключевые слова: информационная живучесть личности; информационное подавление; технологическая доступность; правовые инсайдеры; цифровое рабство.

DIGITAL SLAVERY AS A THREAT TO DIGITAL TRANSFER INDIVIDUALS, SOCIETIES, STATES

Alekseev Anatoly
Saint Petersburg State Maritime Technical University
3 Lotsmanskaya str., Saint Petersburg, 194064, Russia
e-mails: iapbgks@bk.ru

Abstract. The problem is raised and the factors, threats and ways of neutralizing abuses of an organizational and informational nature in modern electronic document management are discussed (EDO) caused by the critical manifestation of the negative properties of the human factor of the EDO operator in the performance of his official duties and abuse of official position, including during the artificial formation by unscrupulous legal entities of various kinds of alleged «debtors» (relevant information incidents) for payment of housing and communal services, especially in terms of RPE, traffic violators, information suppression of various kinds of «complainants» due to the use of «technologies» for mass distribution of e-mails «by cliché,» mass use of virtual informants and answering machines, suppression of information and redundant (without subject matter) and multi-page irresponsible letters. It was concluded that such a «digital bureaucracy» should be considered as a critical threat to the development of EDO, which, in conditions of digital accessibility, massaging EDO flows and legal regulations such as «execution within 5 days after posting a message in a data bank» creates an atmosphere of hopeless «digital slavery» for «informational naked» ordinary citizens. It was

proposed to develop the FZ-152 to create a system of legally significant personal information security system from «legal insiders» from among society and the state.

Keywords: information survivability of the individual; information suppression; technological availability; legal insiders; digital slavery.

Цифровая трансформация личности, общества, государства, не смотря на бесспорные достижения и прогресс, породили наряду с перспективными тенденциями ряд вопросов, которые требуют неотложного внимания и принятия своевременных упреждающих и результативных действий.

Одной из неотложных для решения проблем, по нашему мнению, следует считать порожденную в последнее время проблему «цифрового рабства». Породили ее, тем не менее, такие положительные факторы, как:

– неоспоримая доступность для массового пользователя технологий ЭДО. По существу, исчезла такая непростая профессия, как профессия секретаря, включавшая решение ежедневных задач формирования и печати многочисленных и разнородных документов, включая безусловное владение грамматикой и стилистикой русского языка, этику межличностных взаимоотношений, отношений между юридическими лицами и мн. др. На смену пришло право, возможность и, к сожалению, необходимость каждому сотруднику, руководителю лично решать эту задачу, упрощенно освоив клавиатуру компьютеров и технологию использования принтеров;

– существенно возрос поток ЭДО, как за счет указанной выше доступности, «появившейся любви» рассматривать даже простые вопросы на «юридически значимом документальном уровне», так и резкого возросшего числа юридических лиц с соответствующим аппаратом ЭДО и ряд других позитивных факторов.

Вместе с тем, для резко возросшего круга «самодеятельных секретарей» профессиональные требования и компетенции остались в среднем далеко неосвоенными. Как следствие, резко снизилась культура ЭДО, грамматика и стилистика документов между юридическими, особенно, физическими лицами и, даже, этика. Но еще, более критичным стало снижение уровня правового обеспечения ЭДО, возможность проявления в нем «правовой неуправляемости» и, даже, эмоциональной несдержанности и бесконтрольности.

В свою очередь, отсутствие других регуляторов кроме судов с их естественными и неоперативными сроками реагирования, сложностью подготовительных и исполнительных процедур приводит в ряде случаев к правовой бесконтрольности ЭДО, а для структур силового и административного блоков, даже, к «информационному терроризму» по отношению к ряду групп «простых» граждан, оказывшихся в информационно незащищенном состоянии. Среди этих граждан, соответствующих фактов и «технологий»:

1. Искусственное формирование недобросовестными юридическими лицами разного рода якобы «должников» с сознательно организованными и инициированными соответствующими информационными инцидентами по оплате жилищно-коммунальных услуг, назначении неподтверждаемых документально «долгов» с соответствующими пени, особенно, в части АО «Петроэлектросбыт», «Единый информационно-расчетный центр», использующими свое монопольное положение и «собственные (неаттестованные) технологии». Причем, прямо уклоняясь от рассмотрения конфликтных вопросов в судебном порядке как инициаторы претензий, присваивают себе право «диктата своей «правды» путем назначения штрафных санкций в форме пени.

2. Необоснованно предъявляемые на фоне массированного цифрового потока событий и соответствующего ЭДО претензии с соответствующими стандартными «актами» к якобы «нарушителям правил дорожного движения» без доведения до них регламентированных уведомлений до «нарушителей» и передачи в Федеральную службу исполнительного производства без необходимых в этом случае судебных решений (регламент КРФоАП, ст. 12.9, ч.6) и, даже, фиксации существа нарушения, без составления процессуальных протоколов, а также, даже, неуполномоченными должностными лицами.

3. Информационного подавления недобросовестными юридическими лицами разного рода якобы «жалобщиков» за счет использования «технологий» массовой рассылки электронных писем «по клише», например, о необходимости оплаты недоказанного (спорного) «долга».

4. Массированного использования разнородных виртуальных информаторов и автоответчиков, безответственных по своей сущности (соответствующих «DDoS-информационных атак») без возможности выхода на персонально ответственных сотрудников (неприкрытые «бизнес-хитрости» безответственных компаний), соответствующих компаний и возможности разрешения в ряде случаев элементарных вопросов, «непосильных», даже, для «высоко интеллектуальных» Алис с их технологиями «искусственного» интеллекта.

5. Подавления информационно-избыточными (без предметного рассмотрения) и многостраничными безответственными письмами «цифровых бюрократов», в совершенстве «владеющих» технологиями копирования и манипуляциями шаблонами с целью запутывания элементарных вопросов и откровенного «одурачивания» вынужденных пользователей ЭДО.

6. Целевые мошеннические информационные атаки с использованием «арсенала» технологий обмана, вымогания и кражи денег пользователей электронных банковских карт, оплайн-сервисов и т.п.

Анализ и обсуждение в кругу специалистов по ИБ и кибербезопасности подобных многочисленных факторов и угрозы показывает, что настало время системно подойти к этой социально опасной проблеме, своевременно изыскать пути нейтрализации злоупотреблений организационно-информационного характера в современном электронном документообороте (ЭДО), обусловленные критическим проявлением негативных свойств человеческого фактора оператора ЭДО при выполнении им должностных обязанностей и злоупотреблении служебным положении.

Сделан вывод, что подобную «цифровую бюрократию» следует рассматривать как критическую угрозу развития ЭДО, которая в условиях цифровой доступности, массирования потоков ЭДО и юридических регламентов типа «исполнения в течение 5 дней после размещения сообщения в банке данных» создает для «информационно обнаженных» рядовых граждан обстановку беспросветного «цифрового рабства».

В этой связи предлагается в развитие ФЗ-152 создать систему юридически значимой системы информационной безопасности личности от «правовых инсайдеров» из среды цифровых мошенников.

СПИСОК ЛИТЕРАТУРЫ

1. Кодекс о административных правонарушениях РФ / https://www.consultant.ru/document (дата обращения 30.06.2023).
2. Федеральный закон 152-ФЗ «О персональных данных» с последними изменениями / https://www.kdelo.ru/art/385620-zakon-o-personalnyh (дата обращения 30.06.2023).

УДК 004.056.5

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В БОРЬБЕ С НЕСАНКЦИОНИРОВАННЫМ ДОСТУПОМ: ЗАЩИТА ОТ АТАК, ИСПОЛЬЗУЮЩИХ МЕССЕНДЖЕРЫ СЕТИ ИНТЕРНЕТ

Бобрышов Данил Павлович, Зацепин Илья Сергеевич, Чуваев Константин Игоревич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, лит. А, Санкт-Петербург, 190000, Россия
e-mail: danil.bobryshov@mail.ru, xiluhax@gmail.com, wizeer66@gmail.com

Аннотация. В данной статье описаны различные методы борьбы с несанкционированным взломом информационных систем, посредством использования электронных писем. Описаны приведенные методы и приведены примеры их работы. Перечислены некоторые сервисы, использующие данные методы.

Ключевые слова: DKIM; phishing; домен; искусственный интеллект; машинное обучение.

PROTECT AGAINST PHISHING ATTACKS

Bobryshov Danil, Zacepin Ilya, Chuvaev Konstantin
Saint Petersburg State University of Aerospace Instrumentation,
Bolshaya Morskaya str., 67, lit. A, St. Petersburg, 190000, Russia
e-mail: danil.bobryshov@mail.ru, xiluhax@gmail.com, wizeer66@gmail.com

Abstract. This article describes various methods of combating unauthorized hacking of information systems through the use of e-mails. The above methods are described and examples of their work are given. Some services using these methods are listed.

Keywords: DKIM; phishing; domain; artificial intelligence; machine learning.

На сегодняшний день наблюдается высокий показатель взломов разного рода информационных систем, используя электронные письма. Подобного рода незаконная деятельность является phishing-атакой. Phishing-атаки являются распространенным видом атак цифрового пространства, которые могут привести к утечке личной информации и материальных потерь для пользователя. Для борьбы с phishing-атаками используются как различные автоматические методы, так и средства машинного обучения [1-3].

Phishing-атаки — это вид мошенничества на интернете, при котором злоумышленник пытается получить доступ к личным данным пользователя, используя поддельные электронные письма, веб-сайты или другие электронные формы связи. Целью phishing-атак может быть получение паролей, номеров кредитных карт, адресов и других личных данных. Основная идея phishing-атак состоит в том, что злоумышленник создает поддельную страницу, которая выглядит как настоящая страница логина на сайте банка, электронной почты или социальной сети. Затем он отправляет пользователю электронное письмо с просьбой обновить свои учетные данные на этой странице.

Целью данной научной публикации является изучение разных методов борьбы с несанкционированным взломом устройства, с помощью электронных писем.

Существует несколько рекомендаций для защиты от phishing-атак, которые могут помочь пользователям сохранить свои личные данные в безопасности. Например, пользователям следует быть внимательными при получении электронных писем от незнакомых отправителей. Если письмо содержит просьбу об обновлении личных данных, пользователь должен внимательно проверить URL-адрес страницы, на которую он перенаправляется, и убедиться, что это настоящий сайт. Еще пользователи могут использовать программы антивирусной защиты, которые могут распознавать и блокировать phishing-сайты. Также необходимо регулярно обновлять программное обеспечение своего компьютера и использовать сильные пароли для своих учетных записей. Также, пользователи могут получить дополнительную защиту, используя двухфакторную аутентификацию, которая требует ввода пароля и подтверждения через другой устройство, такое как мобильный телефон.

Существуют разные вспомогательные средства защиты, такие как SPF (Sender Policy Framework) и DKIM (DomainKeys Identified Mail), которые позволяют пользователям проверять подлинность электронных писем и идентифицировать отправителя. SPF позволяет отправителю указывать список доверенных серверов,

которые могут отправлять письма от его имени. DKIM добавляет цифровую подпись к письму, что позволяет получателю проверить, что оно было отправлено именно от того, кто утверждает, что отправил его. Эти технологии настраиваются на уровне домена отправителя, и их использование может помочь пользователям избежать отправки личной информации мошенникам и защитить свои данные.

Машинное обучение на основе обучения «с учителем» является эффективным средством защиты от phishing-атак. Этот подход основывается на использовании большой базы данных phishing-сайтов, чтобы обучить компьютер распознавать их и блокировать пользователей, пытающихся получить доступ к таким сайтам [4].

Средство защиты «Bag-of-words» использует метод, при котором текст представляется в виде совокупности слов, а затем каждое слово преобразуется в числовое значение на основе его частоты в тексте. Эти числовые значения могут быть использованы для обучения модели машинного обучения, которая может распознавать phishing письма и блокировать их.

Байесовские классификаторы — это математический метод, используемый в задачах машинного обучения для классификации данных. Они могут быть применены, в том числе, для защиты от phishing-атак. Для каждого электронного письма вычисляется вероятность, что оно является phishing, и тем самым возможно избежать его случайного открытия и проникновения хакеров в пользовательские данные.

Random Forest — это метод машинного обучения, который часто используется для защиты от phishing-атак. Он основан на создании ансамбля решающих деревьев, каждое из которых производит классификацию, основанную на наборе правил, производимых из обучающей выборки данных.

Deep Learning — это метод машинного обучения, который использует нейронные сети для анализа и обработки больших объемов данных. Этот метод используется многими компаниями для защиты своих систем от фишинговых атак.

В ходе исследования были проанализированы различные методы борьбы с phishing-атаками. Защита от phishing может применяться на разных уровнях, от технического (использование фильтров спама и блокировка доменов) до социального (обучение пользователей узнавать phishing атаки). Одним из эффективных способов борьбы с phishing является использование систем искусственного интеллекта и машинного обучения. Эти системы могут обнаруживать phishing сайты и электронные письма, а также определять аномальное поведение пользователей, что может указывать на подозрительную деятельность.

СПИСОК ЛИТЕРАТУРЫ

1. Судаков А. В., Грамзин А. В., Дудин Д. А. Мошенничество и фишинг в сети // Научно-образовательный журнал для студентов и преподавателей StudNet, 2021. № 6. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/moshennichestvo-i-fishing-v-seti/viewer (дата обращения: 27.06.2023).
2. Афанасьева Н. С., Елизаров Д. А., Мызникова Т. А. Классификация фишинговых атак и меры противодействия им // Инженерный вестник Дона, 2021. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/klassifikatsiya-fishingovyh-atak-i-mery-protivodeystviya-im/viewer (дата обращения: 24.06.2023).
3. Mukhamadieva K. Обзор методов обнаружения фишинговых атак на основе искусственного интеллекта // Вестник ДонНУ : научный журнал. Серия Г: Технические науки, 2021. № 4. [Электронный ресурс]. URL: https://www.researchgate.net/publication/360218773_OBZOR_METODOV_OBNARUZENIA_FISINGOVYH_ATAK_NA_OSNOVE_ISKUSSTVENNOGO_INTELLEKTA (дата обращения: 24.06.2023).
4. Пурисов Д. И., Летникова Е. М. Машинное обучение для определения фишинговых интернет-ресурсов // Международный научный журнал «Синергия Наук», 2021. [Электронный ресурс]. URL: http://synergy-journal.ru/archive/article7459 (дата обращения: 25.06.2023).

УДК 004.418

ЗАДАЧА РАЗРАБОТКИ СЕРВИСА ПЛАНИРОВАНИЯ СТОИМОСТИ АВТОМОБИЛЬНОГО МАРШРУТА С УЧЁТОМ ПОЛЬЗОВАТЕЛЬСКИХ ПАРАМЕТРОВ

Корепанова Анастасия Андреевна, Есин Максим Сергеевич, Сабреков Артём Азатович
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
14 линия, 39, Санкт-Петербург, 199178, Россия
e-mail: aak@dscs.pro, mse@dscs.pro

Аннотация. Данная работа посвящена задаче разработки сервиса планирования экономически выгодного автомобильного маршрута с учётом стоимости дозаправок и пользовательских параметров, отражающих его предпочтения в АЗС. В работе сформулирована актуальность задачи, а также предложен алгоритм её решения.

Ключевые слова: Оптимизация маршрута, расчет стоимости поездки, алгоритм Дейкстры, заправочные станции, стоимость топлива

THE TASK OF DEVELOPING A SERVICE FOR PLANNING THE COST OF A VEHICLE ROUTE TAKEN INTO ACCOUNT OF USER PARAMETERS

Korepanova Anastasia, Esin Maksim, Sabrekov Artem
St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: aak@dscs.pro, mse@dscs.pro

Abstract. This work is devoted to the problem of developing a service for constructing an economical automobile route, taking into account the cost of refueling and parameters reflecting its preferences at gas stations. The work determines the relevance of the problem, and also proposes an algorithm for solving it.

Keywords: Route optimization, trip cost calculation, Dijkstra's algorithm, gas stations, fuel cost.

На сегодняшний день автомобильный туризм является основным способом путешествий россиян [1], увеличение автомобильного турпотока является одной из целей Минэкономразвития до 2030 года [2]. В этих условиях актуальными становятся задачи цифровизации этой сферы туризма, решение которых поспособствует её развитию.

Одной из таких задач является задача оптимизации маршрутов туристов. В то время как задача построения кратчайшего маршрута активно решается навигаторами и прочими сервисами, например, «Яндекс картами», задача оптимизации стоимости маршрута с учётом дозаправок не решена.

Данная работа посвящена постановке задачи разработке сервиса, который способен автоматически строить экономически выгодный маршрут с учетом пользовательских параметров.

Для разработки данного сервиса необходимо решить следующие задачи:

1. Найти источники информации о стоимости топлива.
2. Проработать структуру базы данных, содержащей информацию о заправках.
3. Разработать механизмы сравнения и валидации информации о заправках, полученной из разных источников.
4. Разработать алгоритм оценки стоимости топлива на топливной станции, о которой нет достоверной информации.
5. Разработать алгоритм построения экономически выгодного маршрута.
6. Добавить возможность для пользователя указывать дополнительные параметры и свои предпочтения: фирма заправки, изначальное количество топлива на момент начала маршрута, наличие на заправке кафе, туалета, мойки, насоса, заправщика, зоны для отдыха и т.д.
7. Разработать систему оценки заправки, которая комбинируется из пользовательских отзывов и информации о заправке из внешних источников.

Данные о заправках для сервиса могут быть получены из официальных сервисов АЗС [3-4], а также из сервисов, имеющих партнерские отношения с АЗС [5-6]. В перспективе в данный сервис возможно добавить возможность оценки расхода топлива автомобиля по его марке и модели или WIN-номеру.

В данной работе была поставлена задача разработки сервиса, способного автоматически строить маршрут с учётом стоимость заправки топлива.

Сформулирована актуальность задачи, а также описаны шаги, необходимые для её решения. Реализация сервиса позволит оптимизировать маршруты автомобилистов на дальние расстояния и сделать путешествия более удобными и экономичными.

Работа выполнена в рамках проекта по государственному заданию СПБ ФИЦ РАН СПИИРАН № FFZF-2022-0003; при финансовой поддержке РФФИ, проект №20-07-00839

СПИСОК ЛИТЕРАТУРЫ

1. В отпуск на авто: о чем говорят статистика и эксперты – https://www.atorus.ru/node/50854
2. В России создадут концепцию развития автомобильного туризма https://xn--90aivcdt6dxbc.xn--p1ai/articles/news/v_rossii_sozdadut_kontseptsiyu_razvitiya_avtomobilnogo_turizma/
3. Сеть АЗС «Газпром». — URL: https://www.azsgazprom.ru/ azs-prices/.
4. Сеть АЗС «РосНефть». — URL: https://www.rosneft-azs.ru/ Nasha-set/about.
5. Drivvo – system for managing vehicle fleets, which gives the manager total control over vehicles and drivers. — URL: https://www.drivvo. com/en.
6. FUELUP – технологический топливный онлайн-сервис, который помогает заправлять автомобиль не покидая салона. — URL: https://fuelup.ru/.

УДК 004.418

СИСТЕМА АВТОМАТИЗИРОВАННОГО КОНТРОЛЯ СТАБИЛЬНОСТИ ФУНКЦИОНИРОВАНИЯ СЕРВИСА РАСЧЕТА СТОИМОСТИ ДОСТАВКИ НА ЛОГИСТИЧЕСКОМ ПОРТАЛЕ CARGOTIME.RU

Назарова Полина Андреевна[1], Есин Максим Сергеевич[2], Сабреков Артём Азатович[2]

[1] Академический университет им. Ж.И. Алферова
Хлопина ул., 8, корп. 3, лит. А, Санкт-Петербург, 194021, Россия

[2]СПИИРАН – СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия

e-mails: ktotochra9@gmail.com, mse@dscs.pro, aas@dscs.pro

Аннотация. Освещается концепция автоматизированной системы для отслеживания стабильности функционирования сервиса расчета стоимости доставки на логистическом портале Cargotime.ru.

Ключевые слова: логистика; система автоматического мониторинга; грузоперевозки; сервис расчета стоимости доставки; веб-разработка.

LOGISTICS PORTAL CARGOTIME.RU: AUTOMATION OF MONITORING THE STABILITY OF THE DELIVERY COST CALCULATION SERVICE

Nazarova Polina[1], Esin Maxim[2], Sabrekov Artem[3]
[1] Academic University named after Zh.I. Alferova,
8/3 Hlopina St, St. Petersburg, 194021, Russia
[2]SPIIRAS – SPCRAS
39 14th Line V.I., St, St. Petersburg, 199178, Russia
e-mails: ktotochra9@gmail.com, mse@dscs.pro, aas@dscs.pro

Abstract. The concept of an automated system to monitor the stability of the delivery cost calculation service is discussed in the context of the logistics portal Cargotime.ru.

Keywords: logistics; automated monitoring system; freight transportation; delivery cost calculation service; web development.

В современном цифровом мире онлайн-системы становятся неотъемлемой частью нашей повседневной жизни. В частности, в логистике каждый этап, начиная от управления запасами и отслеживания поставок, заканчивая оптимизацией маршрутов и координацией перевозок, тесно связан с функционированием онлайн-систем. Тем не менее, как и всякая технология, они подвержены возможным сбоям и ситуациям, которые могут нарушить их стабильность и производительность.

Логистический портал Cargotime.ru [1], разрабатываемый на базе лаборатории теоретических и междисциплинарных проблем информатики [2], является одним из примеров таких онлайн-систем. Важную роль на портале играет сервис, служащий для расчета стоимости доставки грузов [3, 4]. Этот инструмент собирает и анализирует данные о стоимости и времени доставки грузов с сайтов различных перевозчиков, представляя информацию в удобном формате на портале Cargotime.ru. Кроме того, сервис позволяет оптимизировать затраты на маршрут, создавая сложные маршруты, где груз перевозится несколькими компаниями, а не одной [5].

Специфика вышеописанного сервиса, обусловленная частым взаимодействием с большим количеством сторонних веб-ресурсов, подразумевает необходимость тщательного контроля за работой сервиса. Таким образом, возникает необходимость создания автоматизированной системы мониторинга, позволяющей снизить риск ошибок и повысить надежность системы.

В условиях жесткой конкуренции в сфере логистики автоматизация мониторинга стабильности работы сервисов играет решающую роль в обеспечении высокого уровня обслуживания клиентов. Исследование системы мониторинга на примере сервиса расчета стоимости доставки на портале Cargotime.ru не только демонстрирует применение современных технологий в логистике, но также открывает путь для дальнейших исследований в области автоматизации и оптимизации логистических систем.

Технические детали и механизмы функционирования описываемой системы могут быть полезны для технических специалистов в сфере логистики и IT. Эта информация может также послужить основой для разработки подобных систем в других сферах бизнеса, делая исследование актуальным для широкой аудитории.

Добавление в систему новых функций, таких как мониторинг производительности и оптимизация запросов к источникам данных, может значительно улучшить систему в перспективе, увеличив ее эффективность и скорость сбора информации.

Такие дополнения могут сделать систему автоматического мониторинга на портале Cargotime.ru мощным инструментом, способным эволюционировать в соответствии с растущими потребностями логистической отрасли.

Система автоматического мониторинга стабильности работы сервиса расчета стоимости доставки грузов на логистическом портале Cargotime.ru играет важную роль в инфраструктуре портала, обеспечивая его стабильную работу. Ее значимость заключается в постоянном контроле и обеспечении надежности сбора и выдачи данных о доставке, что является фундаментальным аспектом эффективного обслуживания клиентов.

СПИСОК ЛИТЕРАТУРЫ

1. Логистический портал Cargotime.ru [Электронный ресурс]. URL: https://cargotime.ru/ (дата обращения: 25.09.2023).
2. Лаборатория теоретических и междисциплинарных проблем информатики [Электронный ресурс]. URL: https://dscs.pro (дата 28.09.2023).
3. Абрамов М. В., Есин М. С. Агрегация сведений и оценка параметров грузовых маршрутов на основе методов машинного обучения в условиях информационного дефицита // Информационная безопасность регионов России (ИББР-2021). XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 27-29 октября 2021 г. : Материалы конференции. СПб : СПОИСУ, 2021. С. 328-330.
4. Калькулятор расчета стоимости доставки на портале Cargotime.ru [Электронный ресурс] URL: https://cargotime.ru/calc/ (дата обращения: 25.09.2023).
5. Есин М. С., Корепанова А. А., Сабреков А. А. Агрегация и анализ сведений логистических компаний для построения сложного маршрута перевозки груза // Программные продукты и системы. Т. 36. 2023. № 2. С. 309-319.

УДК 004.8

ОЦЕНКА СКЛОННОСТИ КОМПОНЕНТОВ ТЕХНИЧЕСКОЙ СИСТЕМЫ К ОТКАЗАМ С УЧЕТОМ ВНЕШНИХ И ВНУТРЕННИХ ФАКТОРОВ ПО ОГРАНИЧЕННЫМ ДАННЫМ ОБ ОШИБКАХ

Столярова Валерия Фуатовна[1], Тулупьев Александр Львович[2]
[1]СПИИРАН – СПб ФИЦ РАН
14 линия, 39, Санкт-Петербург, 199178, Россия
[2]Северо-Западный институт управления – филиал РАНХиГС
Средний проспект В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mails: vfs@dscs.pro

Аннотация. Технические системы часто функционируют в условиях воздействия множества факторов. Одной из составляющих управления такими системами является предиктивное обслуживание их компонент, которое опирается на предсказание отказов системы по разнообразным данным, отражающим ее функционирование. При этом данные об отказах часто бывают ограничены. В работе предлагается использовать существующий подход оценки интенсивности гамма–пуассоновского процесса по ограниченным данным для комплексного моделирования процесса отказов технической системы. Динамические байесовские сеть доверия используются для учета иземенчивости системы во времени и влияния факторов внешней среды.

Ключевые слова: предиктивное обслуживание; интенсивность; неполные данные; динамическая байесовская сеть доверия

ОЦЕНКА СКЛОННОСТИ КОМПОНЕНТОВ ТЕХНИЧЕСКОЙ СИСТЕМЫ К ОТКАЗАМ С УЧЕТОМ ВНЕШНИХ И ВНУТРЕННИХ ФАКТОРОВ ПО ОГРАНИЧЕННЫМ ДАННЫМ ОБ ОШИБКАХ

Stoliarova Valeriia Fuatovna[1], Tulupyev Alexander L'vovich[2]
[1]SPIIRAN-SPb FRC RAS
the 14th Line, 39, St. Petersburg, 199178, Russia
[2]Northwestern Institute of Management - branch of RANEPA
Sredniy prospekt V.O., 57/43, St. Petersburg, 199178, Russia
e-mails: vfs@dscs.pro

Abstract. Technical systems often operate under the influence of many factors. Predictive maintenance of its components is based on the prediction of system failures based on a variety of data reflecting its functioning. At the same time, data on failures are often limited. The paper proposes the existing approach of estimating the intensity of the gamma–Poisson process from limited data for complex modeling of the failure process of a technical system. A dynamic Bayesian belief network is used to account for the variability of the system over time, environmental factors.

Keywords: predictive maintenance; intensity; incomplete data; dynamic Bayesian belief network

Предиктивное обслуживание технических систем получило широкое распространение с развитием концепции Индустрии 4.0 [1, 2], которая предполагает внедрение методов искусственного интеллекта, в частности, для оценки состояния системы. Для решения этой задачи используются исторические данные об отказах системы, а также наблюдения за различными техническими характеристиками ее компонентов. Значительная часть методов, использующихся для определения ключевых для предиктивного обслуживания систем показателей, таких как оставшееся полезное время работы (remaining useful time) и частота отказов системы, управляются данными, т.е. являются data–driven [3]. Так как вероятность является естественным языком анализа риска, поэтому для кумулятивного представления последовательности эпизодов на временной оси используются вероятностные модели, как точечный случайный процесс [4].

Однако при наблюдении за некоторыми системами отказы достаточно редки [3], что затрудняет прямое использование статистических и data–driven методов и оправдывает применение экспертных знаний при моделировании искомых показателей. В отдельных приложениях для оценки частоты отказов системы использовались байесовские сети доверия [5, 6].

В рамках исследования задача оценки показателей предиктивного обслуживания системы (частоты отказов) рассматривается как задача моделирования функции интенсивности точечного процесса отказов системы по ограниченным данным об эпизодах отказов системы с учетом зависящих от времени ковариант. Подобные методы уже использовались в стационарном случае при оценке характеристик рискообразующего поведения индивидов [8]. Особенностью применения таких методов при решении задачи текущего исследования является наличие изменяющихся во времени факторов, отражающих состояние системы в различные моменты времени. Теоретическая значимость исследования заключается в новой структуре динамической байесовской сети, которая позволяет моделировать динамическую зависимость интенсивности гамма–пуассоновского процесса и его ковариант. Практическая значимость исследования состоит в методе оценки интенсивности нестационарного гамма–пуассоновского по неполным данным о вехах процесса с учетом ковариант, зависящих от времени. Предлагаемый в исследовании подход является новым.

В целом, задача восстановления параметров точечных случайных процессов возникает в тех областях знаний, где требуется оценка некоторого кумулятивного показателя, отражающего реализацию эпизодов на

временной оси. В области эпидемиологии при определении риска распространения некоторых инфекций требуется оценка частоты участия в определенных типах поведения [7, 8]. Однако в силу ограниченности ресурсов данные о вехах процессов являются неполными и неточными, например, если при работе с самоотчетами респондетов о произошедших эпизодах [7]. В этом случае для оценки искомого кумулятивного показателя использовались байесовские сети доверия.

Задача оценки кумулятивных характеристик процесса отказов технической системы рассматривается через призму разработанного ранее подхода, позволяющего по данным о нескольких интервалах между эпизодами поведения для нескольких оценивать кумулятивные характеристики . Однако в этом случае необходимо учитывать некоторые особенности предметной области:

- наличие изменяющихся во времени ковариант, отражающих показатели системы;
- малое количество наблюдений — истинных отказов системы;
- наличие запланированного обслуживания компонентов системы.

В рамках текущего исследования для учета перечисленных особенностей предлагается структура динамической байесовской сети. Ключевой переменной, как и в ранее разработанных моделях оценки риска, предлагается использовать параметр функции интенсивности точечного процесса отказов системы. При этом каждый слой сети описывает промежуток времени между двумя отказами компонента системы, с учетом зависящих от времени ковариант, таких как частота обслуживания компонентов системы на каждом этапе и телеметрические показатели работы машины. Ключевой переменной каждого временного слоя динамической байесовской сети является длина интервала между отказами компоненты системы, при условии интенсивности проводимого обслуживания и данных датчиков. Означивания таких ключевых переменных позволяют оценить апостериорную кумулятивную интенсивность отказов компонента системы с учетом проводимого обслуживания. Отметим, что интенсивность планового обслуживания компонентов также может оцениваться с помощью подхода на основе последних эпизодов в случае, когда данные ограничены.

Предложенная структура динамической байесовской сети доверия может использоваться в ситуациях комплексного анализа отказов компонент системы по разнородным, зависящим от времени характеристикам. Особое значение предлагаемые модели имеют в тех областях знаний, где данных об отказах компонент системы мало или в наблюдаемых показателях содержатся ошибки. В этом случае аппарат байесовских сетей доверия позволяет включать в рассуждение экспертную информацию.

СПИСОК ЛИТЕРАТУРЫ

1. Ansari F., Glawar R., Sihn W. Prescriptive maintenance of CPPS by integrating multimodal data with dynamic Bayesian networks //Machine Learning for Cyber Physical Systems: Selected papers from the International Conference ML4CPS 2017. Springer Berlin Heidelberg, 2020. С. 1-8.
2. Zonta T., Da Costa C. A., da Rosa Righi R., de Lima M. J., da Trindade E. S., Li G. P. Predictive maintenance in the Industry 4.0: A systematic literature review //Computers & Industrial Engineering. 2020. Vol. 150. Pp. 106889.
3. Jovicic E., Primorac D., Cupic M., Jovic A. Publicly Available Datasets for Predictive Maintenance in the Energy Sector: A Review // IEEE Access. 2023. Vol 11. Pp. 73505 – 73520
4. Si X. S., Wang W., Hu C. H., Zhou D. H. Remaining useful life estimation–a review on the statistical data driven approaches //European journal of operational research. 2011. Vol 213. No. 1. Pp. 1-14.
5. Zhang Y., Weng W. G. Bayesian network model for buried gas pipeline failure analysis caused by corrosion and external interference //Reliability Engineering & System Safety. 2020. Vol. 203. Pp. 107089.
6. Cai B., Zhang Y., Wang H., Liu Y., Ji R., Gao C., Liu J. Resilience evaluation methodology of engineering systems with dynamic-Bayesian-network-based degradation and maintenance //Reliability Engineering & System Safety. 2021. Vol. 209. Pp. 107464.
7. Пащенко А. Е., Тулупьев А. Л., Тулупьева Т. В., Красносельских Т. В., Соколовский Е. В. Косвенная оценка вероятности заражения ВИЧ-инфекцией на основе данных о последних эпизодах рискованного поведения //Здравоохранение Российской Федерации. 2010. №. 2. С. 32-35.
8. Столярова В. Ф., Торопова А. В., Тулупьев А. Л. Модель для оценки частоты публикации постов в онлайн социальной сети по неполным данным с учетом объективных детерминант поведения //Нечеткие системы и мягкие вычисления. 2021. Т. 16. №. 2. С. 77-95.

УДК 351

РАЗРАБОТКА МЕТОДА ВЫЯВЛЕНИЯ ФЕЙКОВЫХ АККАУНТОВ В СОЦИАЛЬНЫХ СЕТЯХ

Низомутдинов Борис Абдуллохонович
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: boris@itmo.ru

Аннотация. Тезисы представляют обзор пилотного исследования для выявления фейковых аккаунтов в социальных сетях, на основе методов машинного обучения. Фейковые аккаунты могут использоваться для распространения ложной или недостоверной информации, что может привести к панике, массовому недоверию или другим негативным последствиям. Для решения задачи был проведен сбор профилей в активных дискуссиях в социальной сети ВКонтакте, и отобраны подозрительные аккаунты по различным факторам. Результаты выражены в виде базы выявленных аккаунтов, на основе которых можно проводить дальнейшее обучение модели, для автоматизированного поиска ботов и расчета количества фейковых записей в дискуссиях.

Ключевые слова: социальные сети; боты; ВКонтакте; парсинг; фейковые аккаунты.

DEVELOPMENT OF A METHOD FOR DETECTING FAKE ACCOUNTS IN SOCIAL NETWORKS

Nizomutdinov Boris
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
Email: boris@itmo.ru

Abstract. The abstracts provide an overview of a pilot study to identify fake accounts in social networks, based on machine learning methods. Fake accounts can be used to spread false or unreliable information, which can lead to panic, mass distrust or other negative consequences. To solve the problem, profiles were collected in active discussions on the VKontakte social network, and suspicious accounts were selected for various factors. The results are expressed in the form of a database of identified accounts, on the basis of which further training of the model can be carried out, for automated search of bots and calculation of the number of fake entries in discussions.

Keywords: social networks; bots; Vkontakte; parsing; fake accounts.

В предыдущих работах была разработана методика оценки дискурсивных практик в Интернете и анализа онлайн-дискуссий в социальных сетях, был произведен анализ делиберативных свойств на страницах региональных органов власти и «приемных» губернаторов в социальных сетях с использованием автоматизированных методов анализа [1]. Данный подход позволил выявить основные темы, на которые ведутся обсуждения, рассмотрены различия в коммуникативных практиках в социальных сетях и мессенджерах.

Исследование комментариев, размещаемых пользователями в социальных медиа, является важным методом исследования при изучении разных форм гражданского диалога и участия граждан в управлении. Размещение постов в социальных медиа является формой такого диалога, когда происходит не только обмен мнениями на нижнем, индивидуальном коммуникационном уровне, но формируются групповые, солидарности, выражающие общественное мнение различных слоев общества. Понимание таких процессов необходимо для поиска путей повышения эффективности вовлечения граждан в диалог с властью и участия в государственном управлении.

Однако, не изученным остается вопрос, какое количество ботов участвует в таких дискуссиях. Наличие ботов может быть вызвано различными факторами. Точного количества ботов в социальных сетях не существует, так как они могут быть созданы и использованы в разных целях. Однако боты действительно широко распространены в социальных сетях, включая ВКонтакте, Facebook, Instagram, Twitter и другие [2].

В настоящем исследовании под ботом будем понимать аккаунты в социальных сетях, которые созданы с намерением скрыть настоящую личность пользователя или вводить других пользователей в заблуждение, их также называют фейковыми аккаунтами. Фейковые аккаунты могут быть созданы с различными целями, такими как распространение дезинформации, манипулирование общественным мнением, спам, фишинг или нежелательное общение. Существует ряд исследований и методов для выявления ботов в разных социальных сетях, на основе их действий и заполненной информации с применением методов машинного обучения и нейронных сетей [3-4]. Несмотря на наличие хороших результатов, поведение фейковых аккаунтов постоянно меняется и требуется постоянное обновление методов для их поиска.

В данной работе предложен метод для поиска ботов на основе методов машинного обучения. Был выбран метод обучения с учителем. Для решения этой задачи необходимо сформировать базу фейковых аккаунтов. На первом шаге была предпринята попытка поиска готового массива фейковых аккаунтов, для обучения модели, однако, поиск не дал результатов, подобных баз в открытом доступе обнаружено не было. Была предпринята попытка создания собственного набора данных для обучения.

Для формирования собственной базы фейковых профилей необходимо выгрузить общий корпус профилей из популярных сообществ. База должна включать в себя основные показатели профилей, например, дату регистрации, количество фотографий, подписок, друзей. Дополнительно, необходимо оценивать записи пользователей вне профиля, для поисков триггеров, указывающих на бота. После чего можно провести разметку профилей и выявить заведомо подложные аккаунты.

В итоге, признаки, используемые в модели, можно разделить на три группы:

– получаемые из статистики профиля (например, заполненность тех или иных полей, количество постов,
– отклонение по времени создания постов);
– фото на аватаре;
– получаемые из текстов (групп или постов).

Проведено пилотное исследования для формирования базы ботов, чтобы в дальнейшем обучить модель для автоматизированного поиска. Были выбраны дискуссии по резонансным темам «Экология» и «Строительство», которые привлекает большое количество аудитории для обсуждений, отдельные посты имели свыше 1000 комментариев, и дискуссия длилась более 6 месяцев. Гипотеза состоит в том, что к таким темам могут подключаться фейковые аккаунты, для обсуждений, лоббирования своих интересов и других целей. Для проведения исследования использовался автоматизированный парсинг, с применением методов API ВКонтакте.

VK API (Application Programming Interface) — это набор методов и функций, предоставляемых социальной сетью ВКонтакте для взаимодействия с ее функциональностью и данными. API предоставляет разработчикам доступ к различным возможностям ВКонтакте, таким как работа с пользовательскими данными, группами, фотографиями, видео, аудиозаписями и другими элементами социальной сети. С помощью VK API разработчики

могут создавать приложения, которые могут взаимодействовать с аккаунтами пользователей, получать и отправлять сообщения, получать информацию о профилях пользователей и групп, загружать и обрабатывать медиафайлы (фото, видео, аудио), а также выполнять другие действия, доступные через VK API.

В итоге, были выгружены ссылки на профили всех участников дискуссий, а также, текст самих комментариев. Был составлен ряд критериев, применяя которые, запланировано выявлять фейковые аккаунты.

Для ручной разметки был разработан фильтр, который подбирал подозрительные аккаунты:

– фильтр автоматически убирает из выдачи результатов всех «собачек»;
– составлен список стоп слов, которые содержаться на стене профилей (например, «простой заработок», «бизнес без вложений» и другие);
– указан процент репостов (как правило, фейки имеют повышенное количество репостов);
– свежая дата регистрации.

Таким образом, отобран массив аккаунтов, которые потенциально относятся к фейковым. Данный набор позволит обучить модель, для автоматизированного поиска аккаунтов. Например, запланировано обучение на подписках, и текстовых данных, которые содержит профиль. Дополнительно, запланировано дополнение модели распознаванием фотографий. Как правило, фейковые аккаунты не содержат изображения лица, и это тагже является триггером для выявления фейкового аккаунта. Для выявления объектов на изображении запланировано использование. YOLOv4 (You Only Look Once version 4) — это одна из самых современных и мощных моделей для обнаружения объектов на изображениях. YOLOv4 применяет нейронные сети для выполнения быстрого и точного обнаружения объектов в реальном времени. YOLOv4 имеет возможность классифицировать объекты на изображении и определить, отсутствуют ли на нем люди. Однако точность обнаружения может зависеть от обучения модели и качества данных, на которых она обучается. YOLOv4 имеет лучшую производительность по сравнению с предыдущими версиями YOLO и обычно способен точно определить, присутствуют ли люди на фото или нет.

Дополнительный интерес представляют фейковые аккаунты в мессенджере Telegram, например, для изучения дискуссий в комментариях к записям в каналах, однако, их изучение ограничено тем, что профили имеют минимальный набор информации о пользователях. Для анализа аккаунтов Telegram можно использовать только методы текстовой аналитики контента, который публикует в комментариях сам пользователь, при этом нет возможности изучать наполнение профиля.

Результаты, представленные в настоящем докладе, не претендуют на всеобъемлющий статус, призваны в некоторой мере восполнить пробелы других методов. Однако, могут быть использованы для изучения коммуникативных практик пользователей.

Исследование выполнено за счет гранта Российского научного фонда № 22-18-00364 «Институциональная трансформация управления электронным участием в России: исследование региональной специфики» (https://rscf.ru/project/22-18-00364/).

СПИСОК ЛИТЕРАТУРЫ

9. Низомутдинов Б.А., Филатова О.Г. Тестирование методов обработки комментариев из Telegram-каналов и пабликов ВКонтакте для анализа социальных медиа // International Journal of Open Information Technologies. 2023. №5.
10. Williamson W., Scrofani J. Trends in detection and characterization of propaganda bots. Proceedings of the 52nd Hawaii International Conference on.
11. System Sciences. Honolulu, USA, 8–11 January 2019, pp. 7118–7123.
12. Кузьмин В.Н., Менисов А.Б., Шастун И.А. Методический подход к выявлению ботов в социальных сетях на основе специального объединения классификаторов // Бизнес-информатика. 2020. Т. 14. № 3. С. 54–66.
13. Bot and gender detection of Twitter accounts using distortion and LSA / A. Bacciu [et al.] // Conference and Labs of the Evaluation Forum (CLEF 2019). Lugano, Switzerland, 9–12 September 2019. [Электронный ресурс].URL: http://ceur-ws.org/Vol-2380/paper_210.pdf (дата обращение: 26.06.2023).

УДК 51.76

КОГНИТИВНОЕ МОДЕЛИРОВАНИЕ ВЗРЫВООБРАЗНОГО РАСПРОСТРАНЕНИЯ ИНВАЗИВНОЙ ИНФОРМАЦИИ В НЕСТАБИЛЬНОМ СОЦИУМЕ

Переварюха Андрей Юрьевич, Манвелова Александра Борисовна, Трофимова Инна Владимировна
Михайлов Владимир Валентинович, Хасанов Дмитрий Салимович
СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
email: madelf@rambler.ru, abmanvelova@mail.ru, i.trofimova@spbu.ru,
mwwcari@mail.ru, khasanovsuai@yandex.ru

Аннотация. Авторами разработан структурно-логический метод модельного проектирования информационных потоков для синхронизации взаимодействующих гибридных вычислительных структур для моделей экстремальных изменений. Метод применен для анализа процессов при вбрасывании агрессивной информации в нестабильный социум и оценки реакции групп общества. Гибридная система развивается на основе формализма когнитивных графов, где концептам вершин сопоставлены системы дифференциальных уравнений. Дугам когнитивного графа заданы условия переопределения правых частей уравнений, соответствующих событиям целенаправленного вброса агрессивной, вызывающей ответную реакцию информации. Структура вычислительного графа на основе экспертных оценок ситуации дополнена условиями, позволивших выделить события агрессивной

инвазии в среде противоборствующих информационных потоков. Алгоритмическая структура изменений графа анализируется как импульсный процесс между вершинами, разделяющий ламинарное функционирование потоков информации и катастрофический режим, сопутствующий распространению и затуханию инвазивных информационных волн в нестабильном социуме.

Ключевые слова: когнитивные модели; кризис потоков информации; анализ эффектов вброса, информационный коллапс; инвазионные процессы в обществе; экстремальные состояния.

APPLICATION OF LOGIC-EVENT MODELING TO DESCRIBE CRITICAL PHASES OF DEVELOPMENT OF SOCIO-INFORMATION PROCESSES

Perevaryukha Andrey, Manvelova Aleksandra, Trofimova Inna, Mikhailov Vladimir, Hasanov Dmitry
SPCRAS
39 14 line V. I., St. Petersburg, 199178, Russia
email: madelf@rambler.ru, abmanvelova@mail.ru, i.trofimova@spbu.ru, mwwcari@mail.ru, khasanovsuai@yandex.ru

Abstract: The authors have developed a structural-logical method of model design of information flows to synchronize interacting hybrid computing structures for models of extreme changes. The method is used to analyze the processes of throwing aggressive information into an unstable society and assess the reaction of social groups. The hybrid system is developed on the basis of the formalism of cognitive graphs, where the concepts of vertices are associated with systems of differential equations. The arcs of the cognitive graph are given conditions for redefining the right-hand sides of the equations corresponding to the events of information injection. The structure of the computational graph, based on expert assessments of the situation, was supplemented with conditions that made it possible to identify the events of aggressive invasion in the environment of opposing information flows. The algorithmic structure of graph changes is analyzed as impulse process between vertices, separating the laminar functioning of information flows and the catastrophic regime accompanying propagation and attenuation of invasive information waves in society.

Keywords: cognitive models; information flow crisis; analysis of stuffing effects, information collapse; invasive processes in society; extreme conditions.

Когнитивные и структурно-логические методы моделирования развиваются нами для анализа последствий информационных инвазий. Исследуются ситуации взрывообразных «эруптивных» фаз развития информационных процессов в современном социуме при замедленной реакции регулирующих организаций. Гибридные вычислительные структуры призваны решать актуальные задачи прогнозирования, качественной и количественной оценки последствий и выработке методов противодействия явлению вторжения целенаправленной деструктивной информации, имеющей тенденцию к неконтролируемому распространению в создавшихся условиях. Смена фаз генезиса и формализация масштабных нестационарных состояний в информационных потоках, к которым относится подавляющее большинство деструктивных информационных вбросов, одновременно одна из актуальных нерешенных проблем для математической социологии как междисциплинарного научного направления. С точки зрения системной социологии постановка задачи формального описания стремительных изменений в информационной динамике у разных общественных групп влияния представляет теоретический интерес из-за необходимой модификации представлений о действующих механизмах, точнее о диапазонах их действия и выключения, в регуляции эффективности передачи волны сообщений в различных состояниях настроения общества.

Процесс распространения волны информационного вброса сравним с агрессивной инвазией. Экодинамика популяций вселенцев зависит от уровня сопротивления биотического окружения. Многие наблюдаемые ситуации при массовых размножениях связаны с явлениями инвазий и адаптаций чужеродных видов перманентной современной проблемой. В некоторых случаях вид-вселенец, представленный изначально малой группой особей, не встречает конкурентного противодействия со стороны автохтонного биологического окружения. Тогда у образующейся популяции происходит максимизация репродуктивного потенциала, который на самом деле является агрегированной и отнюдь не независимой характеристикой. Данная характеристика должна включать запаздывание в регуляции. Инвазия далеко не всегда переходит в стадию вспышки. В некоторых случаях инвазия может оказаться даже полезной для питания ценных потребителей, как в случае с донной фауной Каспийского моря, где проникновение средиземноморских моллюсков повысило продуктивность кормовой биомассы рыб во время падения уровня моря. Вспышки численности свойственны и неизмеримо давно присутствующим в экосистеме видам. В некотором смысле они становятся частью круга последовательных перестроений в растительных сообществах. О цикличности или стохастичности причин таких явлений ведется длительная дискуссия. Можно сделать вывод о действии пороговых состояний численности при сложном межвидовом взаимодействии группы видов, составляющих трехуровневую систему противоборства ос-паразитов и их жертв, других ос или фитофагов. Информационные процессы развиваются по принципам инвазий — резкая вспышка переходит в активный колебательный режим с затуханием волн.

Основной аспект, выделяемый нами в комплексной проблеме исследования вспышек в том, что по-видимому, нереально выделить общий путь развития процесса именно с позиций теории метаморфозов фазовых портретов нелинейных динамических систем, аппарата для описания резких изменений. Данные ряда примеров указывают на различия в типах бифуркаций. Наиболее оправданным видится сценарный подход к моделированию ситуаций с некоторым множеством вариантов дальнейшего развития. Мы предлагаем

непрерывную модель бифуркационного запуска сценария специфически осциллирующей вспышки информационной волны на основе концепции запаздывания в действии регулирующих факторов. В биосистемах известны аналогичные явления. Модельный сценарий в графе актуален по имеющимся данным наблюдений для случаев поражения вредителем площадей опытных участков и позволяет оценивать временную эволюцию характеристик пилообразных колебаний, аналогичных графикам информационных явлений. Традиционными методами математической экологии описать нелинейность завершения и спонтанность выхода из хаотических флуктуаций представлялось невозможным. Выбран подход в форме непрерывно-дискретной динамической системы, строившейся на формализации выживаемости поколения. Изменения непрерывной системы в выделенные условиями моменты времени были соотнесены с переходами между тремя стадиями развития процесса информационного кризиса. Непрерывная часть базовой модели для $N(t)$ описывалась переопределяемой правой частью дифференциального уравнения для убыли информационной активности на трех последовательных временных интервалах с набором условий завершения активности инвазионной волны [2]. Получили сложную графовую зависимость для дискретной составляющей траектории, которая демонстрирует спонтанное преодоление порогового равновесия из переходного хаотического режима. Для описания завершения информационной вспышки инкапсулирован триггерный функционал. Порог запуска агрессивной вспышки информационного вброса при задействовании L информационных каналов не может быть монотонно достижим из любого состояния системы [3] Потому несвязные границы областей притяжения аттракторов в нашей модели хорошо описывают данный аспект информационного противоборства. Существование порога числа информационных каналов, отраженного в модели граничным неустойчивым положением равновесия, объясняется сложными взаимоотношениями различных трендов. Полученные модели можно использовать в составе систем уравнений для оценки явного информационного противоборства [4].

Волна инвазионной информации после стремительной вспышки может проходить критическое состояние с сохранением остаточного информационного шлейфа, либо полным исчезновением шума из возмущенного информационным вбросом социума. Полученный в уравнении переходный режим можно рассматривать так же для задачи анализа случая специфического развития рецидивирующей информационной атаки и запуска деструктивной самоподдерживающейся цепной реакции нагнетания кризиса [5], часто называемой паника. Проводим расширение уравнений для модельных исследований информационных процессов со сложным независимым противодействием. Спровоцировать следующую серию колебаний информационных потоков в такой модели может стремительные изменения состояния общественных настроений. В дальнейшем развитии модели нами планируется описание осциллирующей пилообразной динамики информационных волн из-за рецидивов активации интереса к деструктивной информации со стороны малых, но активных групп влияния.

Работа выполнена коллективом по проекту РНФ № 23-21-00339 (в СПБ ФИЦ РАН).

СПИСОК ЛИТЕРАТУРЫ

1. Дубровская В. А. О критериях обоснованности для анализа нелинейных эффектов в моделях эксплуатируемых популяций // Проблемы механики и управления: Нелинейные динамические системы. П., 2016. № 48. С. 74-83.
2. Переварюха А. Ю. Модель развития спонтанной вспышки численности насекомого с апериодической динамикой // Энтомологическое обозрение. СПб., 2015. Т. 94. № 1. С. 203-215.
3. Борисова Т. Ю., Соловьева И. В. Проблемные аспекты моделирования популяционных процессов и критерии их согласования // Математические машины и системы. К., 2017. № 1. С. 71-81.
4. Дубровская В. А., Переварюха А. Ю., Трофимова И. В. Модель динамики структурированных субпопуляций осетровых рыб Каспия с учетом отклонений в темпах развития молоди // Журнал Белорусского государственного университета. Биология. М., 2017. № 3. С. 76-86.
5. Переварюха А. Ю. Итерационная непрерывно-событийная модель вспышки численности полужесткокрылого фитофага // Биофизика. М., 2016. Т. 61. № 2. С. 395-404.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

УДК 004.654

ПРИМЕНЕНИЕ МЕТОДОВ КОМПЬЮТЕРНОЙ МАТЕМАТИКИ И КРАТНОМАСШТАБНОГО АНАЛИЗА ДЛЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Бортникер Петр Владимирович, Саенко Игорь Борисович
СПИИРАН – СПб ФИЦ РАН
14-я линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mails: bort29@mail.ru, ibsaen@mail.ru

Аннотация. Рассматривается методика обнаружения вторжений в компьютерные сети посредством моделирования сигналов в среде MATLAB с последующим их разложением по базису вейвлетов. Проведён сравнительный анализ полученных массивов вейвлет-коэффициентов.

Ключевые слова: компьютерные помехи; обработка сигналов; шумовая компонента; вейвлет-разложение.

APPLICATION OF METHODS OF COMPUTER MATHEMATICS AND MULTISCALE ANALYSIS TO DETECT INTRUSIONS INTO INFORMATION SYSTEMS

Peter Bortniker, Igor Saenko
SPIIRAS – SPCRAS
39 14th line of V. I., St. Petersburg, 194178, Russia
e-mails: bort29@mail.ru, ibsaen@mail.ru

Abstract. A technique for detecting intrusions into computer networks by modeling signals in the MATLAB system with their subsequent decomposition according to the wavelet basis is considered. A comparative analysis of the obtained arrays of wavelet coefficients is carried out.

Keywords: computer interference; signal processing; noise component; wavelet decomposition.

Обнаружение вторжений и сетевая безопасность стали важной проблемой в современном мире [1, 2]. Сетевые вторжения осуществляются в различных формах: вирусы, рассылка спама, черви, вредоносное ПО, повышение привилегий, несанкционированный вход в систему, доступ к конфиденциальной информации, атаки на уязвимые службы, внедрение нежелательных пакетов в целевые сети. Как следствие, эта небезопасная среда привела к развитию систем обнаружения сетевых вторжений (NIDS). Система обнаружения вторжений — это программный инструмент, который собирает и анализирует информацию о хосте или сети для выявления атак, которые пытаются поставить под угрозу целостность, доступность или конфиденциальность системы/сети. Методы, основанные на вейвлет-преобразовании, в последнее время широко используются в NIDS.

Вейвлет-анализ и обработка сигналов на сегодняшний день — быстро развивающаяся область прикладной науки, которая в будущем может стать ведущим способом обработки информации. На основе вейвлет-преобразования могут основываться не только методы обнаружения вторжений, но также и высокоэффективные алгоритмы сжатия информации, что очень актуально в наши дни. Вейвлет-анализ имеет применение во многих областях фундаментальных исследований, включая медицину, инженерное дело и финансы. За последние полтора года большинство исследований, связанных с вейвлетами были посвящены применению вейвлетов в таких областях как стеганография и стегоанализ, распознавание голоса и образов, анализ сетевых атак и защита нейросетей [3, 4].

В случае обнаружения вторжений в информационные системы вейвлет-анализ, позволяет при грамотном подборе параметров для исследования с высокой вероятностью определить аномалии сетевого трафика. Вейвлет-анализ относится к поведенческим методам. С этой целью часто используют возможности математического пакета Wavelet Toolbox MATLAB для анализа сигналов, очистки от шума и сжатия [5, 6].

В проведённом исследовании с помощью математического пакета Wavelet Toolbox MATLAB была выполнена генерация двух сигналов. Эталонный сигнал содержал 4 гармоники, ко второму был добавлен белый шум с уровнем 10% от среднеквадратичного значения сигнала. Оба сигнала были разложены по базису вейвлетов db2.

Результаты показали, что вейвлет-представление, как и представление Фурье, содержит число значимых компонент, пропорциональное числу гармоник сигнала. В результате выполнения программы были получены значения коэффициентов вейвлета, количеством, равным количеству отсчетов сигнала.

Получены массивы вейвлет-коэффициентов для исходного и зашумленного сигналов соответственно. Выполнена статистическая обработка полученных результатов. Обнаружено, что вейвлет-преобразование исходного и зашумленного сигнала имеет сходную огибающую, однако, за счет шумовой компоненты, наблюдаются значительные отклонения отдельных коэффициентов. В дальнейшем планируется выполнить проверку статистической гипотезы о значимости различий параметров распределения.

Для получения количественных характеристик был получен энергетический спектр сигнала, восстановленного по вейвлет-коэффициентам. Для данного энергетического спектра была вычислена кумулята энергии на высоких, средних и низких частотах.

После проведения вейвлет-анализа нормального сетевого трафика, принятого за эталонный сигнал и вейвлет-анализа сетевого трафика, полученного в момент симуляции атаки, было обнаружено следующее: значение кумуляты энергии сетевого трафика, полученного в момент симуляции атаки, значительно превышает значение кумуляты энергии эталонного сигнала. И на высокой, и на средней, и на низкой частоте получено различие в значениях кумулят в среднем на 2 порядка. Этот факт позволяет обнаружить вторжение на раннем этапе и принять соответствующие меры по его предотвращению. Также это позволяет понять, на какой стадии находится атака, если ее не получилось обнаружить в начале. Сравнительный анализ кумулят энергии эталонного и атакуемого сигнала показывает, что наименьшее отношение наблюдается на средней частоте.

Следовательно, можно предположить, что отношение кумулят энергии в 100-150 раз может являться очевидным признаком наличия вторжения. Однако, данное предположение нуждается в дальнейшей проверке и требует наличия большого количества опытных данных.

СПИСОК ЛИТЕРАТУРЫ

1. Salagean M. Real network traffic anomaly detection based on analytical discrete wavelet transform // 2010 12th International Conference on Optimization of Electrical and Electronic Equipment. IEEE, 2010. С. 926-931.
2. Ильичева В. В., Порческо П. М. Исследование современных подходов к обеспечению сетевой безопасности // Труды Ростовского государственного университета путей сообщения. 2019. №. 4. С. 48-52.
3. Дудникова А. И. Разработка системы мониторинга и анализа сетевых потоков с применением алгоритма вейвлет-преобразований // Перспектива-2021: Материалы IX Всероссийской молодежной школы-семинара по проблемам информационной безопасности. М.: ИД Академия Естествознания, 2022. С. 100-103.
4. Фомичева В. А., Паротькин Н. Ю. Обзор технологий обеспечения безопасности функционирования IoT-устройств // Актуальные проблемы авиации и космонавтики 2022. Том 2. С. 318-320.
5. Шелухин О.И., Рыбаков С.Ю. Ванюшина А.В. Модификация алгоритма обнаружения сетевых атак методом фиксации скачков фрактальной размерности в режиме online // Труды учебных заведений связи. 2022. Т. 8. № 3. С. 117-126.
6. Хамухин А. А. Совмещение вычисления интегрального вейвлет-спектра и непрерывного вейвлет-преобразования в задаче обнаружения узкополосных шумовых сигналов // Системы анализа и обработки данных. 2014. №. 2 (55). С. 77-85.

УДК 004.738

ОПИСАНИЕ ТЕХНОЛОГИИ РАСПОЗНАВАНИЯ ОБРАЗОВ ПРИ ВЫЯВЛЕНИИ ДОРОЖНО-ТРАНСПОРТНЫХ ПРОИСШЕСТВИЙ

Галеева Евгения Алексеевна
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mail: zenagaleeva1315@gmail.com

Аннотация. Рассматриваются известные методы распознавания объектов и классификации объектов в зависимости от обстоятельств, применяемые при обнаружении дорожно-транспортных происшествий и чрезвычайных ситуация на дорогах.

Ключевые слова: компьютерное зрение; нейронные сети; киберфизические системы; ДТП.

DESCRIPTION OF PATTERN RECOGNITION TECHNOLOGY FOR DETECTING ROAD ACCIDENTS

Galeeva Evgenia
Saint Petersburg State University of Aerospace Instrumentation
67, Bolshaya Morskaya St, St. Petersburg, 190121 Russia
email: zenagaleeva1315@gmail.com

Abstract. Known methods of object recognition and classification of objects depending on circumstances, applied in detection of traffic accidents and emergency situations on roads, are considered.

Keywords: computer vision; neural networks; cyber-physical systems; road accidents.

На данный момент активное практическое применение искусственного интеллекта в сфере дорожно-транспортных событий известно в городе Москве. На протяжении пяти лет нейронные сети помогают инспекторам обнаруживать нарушения и в разы быстрее на них реагировать [1].

Так же в Перми, компания TrafficData разработала систему, распознающую аварии на дорогах, по средствам обнаружения определённых параметров аварии: скорость транспорта сильно отклоняется от средней скорости на данном промежутке дороги, воспламенение, задымление, появление и поведение людей, не стандартное для данного участка дороги. Нейронная сеть помогает быстрее обнаружить и среагировать

на аварию специальным службам, что означает уменьшение количества пробок из-за аварий, своевременная помощь пострадавшим при аварии [2].

Для реализации модуля для распознавания дорожно-транспортных происшествий, в первую очередь необходимо на потоке видео отделить машины от других объектов. Далее в действие вступает алгоритм, вычисляющий нормальные условия в определённый промежуток времени для определённого участка дороги, будь то перекрёсток, регулируемы по средствам светофора, или участок высокоскоростной трассы. Алгоритм должен запоминать нормальные условия и выделять объекты, сильно отклоняющийся от средних значений участка. После работает нейронная сеть, определяющая признаки ДТП: повреждение машин, воспламенение, соприкосновение машин и другие признаки. Если программа обнаруживает признаки аварии, то поступает сигнал специальным службам, где диспетчер решает, как отреагировать на данное дорожное происшествие.

Среднее значение движения на участках дороги высчитывается при помощи метода межкадровой разницы, по которой определяется движение машины на определённое расстояние за определённый промежуток времени [3]. Признаки аварии будут определяться по средствам метода обнаружения объектов (Object detection) и при наличии определённых наборов объектов, будет выявляться авария ли это [4].

При обработке видео информации необходимо выявлять среднее значение скорости движения на участке дороги, требуется весь описанный выше алгоритм. При обработке же статической фото-информации достаточно использовать нейронную сеть только для выявления признаков аварии.

СПИСОК ЛИТЕРАТУРЫ

1. Блог компании TrafficData [Электронный ресурс]. URL: https://trafficdata.ru/about-us/ (дата обращения 17.09.2023).
2. Чуйков Р. Ю., Юдин Д. А. Обнаружение транспортных средств на изображениях загородных шоссе на основе метода Single Shot MultiBox Detector // Научный результат. Информационные технологии. Т. 2. № 4. 2017. С. 50-58.
3. Ненашев В. А. Компьютерное зрение Анализ, обработка и моделирование. Учебное пособие. 2022. 78 с.
4. Юдин Д. А., Горшкова Н. Г., Кныш А. С., Фролов С. В. Распознавание транспортных средств и регистрация их траектории движения на последовательности изображений // Вестник БГТУ им. В.Г. Шухова. 2016. № 6. С. 139-148.

УДК 004.738

РАСПОЗНАВАНИЕ ДОРОЖНО-ТРАНСПОРТНЫХ ПРОИСШЕСТВИЙ С ПОМОЩЬЮ КОМПЬЮТЕРНОГО ЗРЕНИЯ

Головкин Матвей Максимович
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mail: matvey.golovkin@mail.ru

Аннотация. Рассматриваются известные способы обнаружения дорожно-транспортных происшествий на дорогах России. Производится поиск аналогов данного продукта в г. Санкт-Петербург. Анализируются компании с малой и средней капитализацией, предоставляющие данные услуги на территории Российской Федерации.

Ключевые слова: искусственная нейронная сеть; дорожно-транспортное происшествие; компьютерное зрение; распознавание образов; киберфизические системы; умный город; безопасный город.

RECOGNIZING ACCIDENTS USING COMPUTER VISION

Golovkin Matvey
Saint Petersburg State University of Aerospace Instrumentation
67 Bolshaya Morskaya St, St. Petersburg, 190121 Russia
email: matvey.golovkin@mail.ru

Abstract. There are consider, that known ways of detecting traffic accidents on the roads of Russia. It is make the search for analogs of this product in St. Petersburg. There are analyze companies with small and medium capitalization providing these services in the territory of the Russian Federation**.**

Keywords: neural network; traffic accident; computer vision; detection; cyber physical systems; smart city; safe city.

Компьютерное зрение в настоящее время является быстро развивающейся областью научных и прикладных исследований.

Назначение компьютерного зрения заключается в формировании полезных выводов относительно объектов и сцен реального мира на основе анализа изображений, полученных с помощью датчиков. При этом обработка видеоинформации осуществляется на универсальных или специализированных компьютерах.

Компьютерное зрение находит применение во многих отраслях, таких как медицина, автомобильная промышленность, безопасность и других.

Существует множество методов компьютерного зрения, которые используются для обработки и анализа изображений. Некоторые из них включают: фильтрацию, сегментацию, распознавание образов, оптическое распознавание символов, детектирование объектов, измерение объектов. Также компьютерное зрение имеет большой потенциал для автоматизации процессов и улучшения качества жизни людей.

Целью реализуемого проекта является уменьшение количества пробок на дорогах г. Санкт-Петербурга благодаря более быстрому реагированию специальных служб на возникающие дорожные происшествия.

Реализации поставленной цели способствует решение следующих задач:

1) Сформировать обучающую выборку из разных категорий дорожно-транспортных происшествий, включая процесс предобработки данных: очистку, нормализацию, кодирование.

2) Выбрать и изучить библиотеки компьютерного зрения и анализа данных.

3) Обосновать архитектуру нейронной сети для решения задачи компьютерного зрения.

4) Разработать приложение для умной камеры, решающей задачу распознавания дорожно-транспортных происшествий.

5) Провести натурный эксперимент.

В настоящий момент известны две компании в России, занимающиеся распознаванием дорожно-транспортных происшествий с помощью компьютерного зрения.

Первая — это Magnus-tech, которая сначала пыталась реализовать данный проект без использования обучающей выборки, но низкая точность распознавания все же подвигла компанию использовать стратегию обучения с учителем. Magnus-tech запустила свою систему распознавания дорожно-транспортных происшествий в четырёх регионах России: Архангельске, Курске, Саратове, Волгограде.

Второй компанией, реализующей технологию компьютерного зрения в системе умного города, является TrafficData, компания была основана в Перми. Разработки TrafficData используют в Москве, Санкт-Петербурге, Перми, Тюмени, Тобольске, Воронеже, Иркутске, Салехарде, Хабаровске, на дорогах Израиля, Бразилии, Турции и Узбекистана, в научных целях − университеты Белоруссии и Таджикистана.

СПИСОК ЛИТЕРАТУРЫ

1. Потапов А. С. Системы компьютерного зрения. СПб. : Университет ИТМО, 2016. 161 с.
2. Вьюгин В. В. Математические основы машинного обучения и прогнозирования. М.: МЦМНО, 2014. 304 с.
3. Блог компании Magnus Tech[электронный ресурс]. URL: https://habr.com/ru/companies/magnus-tech/articles/738836/ (дата обращения 19.09.2023).
4. Блог компании TrafficData [Электронный ресурс].URL: https://trafficdata.ru/about-us/ (дата обращения 17.09.2023).

УДК 004.056

МЕТОД СИМБИОТИЧЕСКОГО ВЗАИМОДЕЙСТВИЯ НЕЙРОННЫХ СЕТЕЙ С ОТСУТСТВИЕМ ЭЛЕМЕНТОВ АНТАГОНИСТИЧЕСКОЙ ИГРЫ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ НАБОРОВ ДАННЫХ

Гололобов Никита Вячеславович, Павленко Евгений Юрьевич
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 194064, Россия
e-mails: gololobov.nv@edu.spbstu.ru, pavlenko_eyu@spbstu.ru

Аннотация. Рассматривается метод симбиотического взаимодействия нейронных сетей на основе установки коэффициентов поощрения по результатам обработки кадра данных, обеспечивающий безопасность наборов данных как на этапе очистки наборов, так и на этапе их верификации.

Ключевые слова: нейронные сети; очистка данных; кибербезопасность; защита наборов данных; машинное обучение; верификация наборов данных.

METHOD SYMBIOTIC OF INTERACTION OF NEURAL NETWORKS WITH NO ANTAGONISTIC GAME ELEMENTS IN PROBLEMS OF ENSURING THE SECURITY OF DATA SETS

Gololobov Nikita, Pavlenko Evgeniy
Peter the Great St. Petersburg Polytechnic University
Russia, 195251, St. Petersburg, Polytechnicheskaya, 29, St. Petersburg, 194064, Russia
e-mails: gololobov.nv@edu.spbstu.ru, pavlenko_eyu@spbstu.ru

Abstract. A method of symbiotic interaction of neural networks is considered based on the setting of incentive coefficients based on the results of processing a data frame, which ensures the safety of data sets both at the stage of cleaning the sets and at the stage of their verification.

Keywords: neural networks; data cleaning; cybersecurity; protection of data sets; machine learning; verification of data sets.

Алгоритмы машинного обучения обеспечивают сбор, накопление, хранение и анализ данных, а результатом их работы может быть решение задачи, нахождение которого иными способами было невозможно. В настоящее время эти инструменты используются для оценки состояния киберфизической системы посредством обработки сырых данных в классифицированные или кластеризованные. Кроме этого, машинное обучение предлагает различные инструменты для понимания сложных данных путем сегментации и упрощения, в том числе оно позволяет не только принимать лучшие решения на основе упорядоченных данных, но и в достаточной мере автоматизировать бизнес-задачи.

Современные методы обеспечения кибербезопасности используют технологии машинного обучения для повышения эффективности выявления и распознавания киберугроз. Одной из существующих проблем использования машинного обучения является чистота и корректность данных, на основе которых производится

обучение нейронных сетей. На данные характеристики набора могут влиять выбросы, неточные, поврежденные, несогласованные или неинформативные данные [1].

Актуальность исследований обоснована растущими объемами и разнородностью данных, которые могут быть использованы для обучения нейронных сетей, а также потребностью в обеспечении кибербезопасности средств, использующих технологии машинного обучения [2]. Кроме этого, результаты исследования могут быть использованы в аналитических системах для повышения показателей чистоты наборов данных, выделения и нейтрализации некорректных записей или кортежей.

Новизна работы заключается в создании симбиотического метода взаимодействия нейронных сетей с отсутствием элементов антагонистической игры на этапе обучения. Научная значимость проводимых исследований заключается в создании новой архитектуры взаимодействия нейронных сетей для обработки разнородных данных.

Результаты проведенных исследований могут быть применены для сокращения объемов человеческих ресурсов, используемых при обработке данных. Объектом исследований являются искусственные нейронные сети, включая способ их взаимодействия между собой. Предметом исследований являются методы очистки данных, которые могут быть применены при обеспечении симбиотического взаимодействия нейронных сетей на этапе обучения.

Общий алгоритм работы очищающей нейронной сети заключается в последовательном исполнении ряда алгоритмов в соответствии с этапами. На первом этапе основной задачей очищающей нейронной сети является классификация типа отравления. На втором этапе в зависимости от результата классификации очищающая нейронная сеть применяет один из алгоритмов очистки данных, накапливает заданное количество записей и передает их в верифицирующую сеть.

По результатам работы верифицирующей сети, принцип которой описан далее, очищающая сеть устанавливает верифицирующей сети поощрительный балл в зависимости от степени разнообразия, вычисляемой посредством коэффициента Джинни, результирующего набора [3]. При поддержании высокого уровня разнообразия устанавливается более высокий поощрительный балл, в противном случае более низкий.

Верифицирующая нейронная сеть получает на вход очищенный фрагмент набора данных и производит расчет его статистических характеристик, а также оценку его влияния на статистические характеристики при внесении в результирующий набор данных. При расчете и оценке вычисляются среднее значение, дисперсия и корреляция полученного фрагмента и результирующего набора [4, 5].

При превышении абсолютной допустимой границы изменения статистических характеристик, верифицирующая нейронная сеть принимает решение о необходимости доработке фрагмента и устанавливает пониженный поощряющий балл очищающей модели. Если пороговые значения не были достигнуты, фрагмент добавляется к результирующему набору, а очищающая нейронная сеть получает повышенный поощряющий балл.

Для снижения воздействия негативных факторов на качестве очищенного набора при очистке должны применяться поощрительные коэффициенты, которые позволят корректировать работу нейронных сетей. При этом такие коэффициенты должны рассчитываться динамически самими нейронными сетями и устанавливаться друг для друга [6, 7]. Предлагаемая модель очистки данных основывается на симбиотических отношении двух нейронных сетей с долгой краткосрочной памятью N_1 и N_2 и справедлива для числовых типов записей. Записи e из набора S, подаваемые на вход нейронной сети N_1, предварительно не размечены. В ходе своей работы N_1 применяет метод очистки m из множества методов очистки M [8] к тем данным, которые классифицированы ей как отравленные, и передает результат нейронной сети N_2.

Нейронная сеть N_2 в свою очередь оценивает влияние новой записи на разнообразие набора G и на основе этой оценки принимает решение о включении записи в результирующий набор. По прошествии заданного количества итераций t нейронные сети N_1 и N_2 устанавливают поощрительные коэффициенты k_1 и k_2, на основании которых корректируется их работа.

Коэффициент k_1 для нейронной сети N_1 устанавливается исходя из степени изменения множества статистических характеристик — значение коэффициента тем меньше, чем больше изменились значения среднего, дисперсии и корреляции в наборе с учетом выхода за пороговое допустимое значение изменений. Использование статистических характеристик набора для оценки корректности очистки позволяет исключить контекстную зависимость, что в свою очередь положительно сказывается на унификации метода для его применения в отношении разнородных наборов данных.

Коэффициент k_2 для нейронной сети N_2 устанавливается исходя из степени изменения значения разнообразия набора данных после включения ряда записей в очищенный набор. При расчете коэффициента k_2 используется коэффициент Джини в качестве меры разнообразия. Его использование позволяет сравнивать распределение значений атрибутов набора данных в совокупностях с различным числом атрибутов при очистке подобных наборов данных, полученных из различных источников.

Таким образом, использование метода симбиотического взаимодействия позволяет сократить объемы человеческих ресурсов, используемых при обработке данных, что в свою очередь может удешевить процесс обработки данных. Метод симбиотического взаимодействия является перспективным не только в контексте очистки данных, но и в контексте машинного обучения в сфере информационной безопасности [9]. Дальнейшие исследования должны быть направлены на разработку способов взаимодействия ансамблей нейронных сетей

в задачах очистки наборов данных, а также на поиск альтернативных методов взаимодействия нейронных сетей с целью определения наиболее перспективного в прикладных задачах подхода.

СПИСОК ЛИТЕРАТУРЫ

1. Coprotector: Protect open-source code against unauthorized training usage with data poisoning / Sun Z. [et al.] //Proceedings of the ACM Web Conference 2022. 2022. С. 652-660.
2. Robust Electricity Theft Detection against Data Poisoning Attacks in Smart Grids // IEEE Transactions on Smart Grid. 2021. Vol. 12. № 3. P. 2675-2684.
3. Zhou H., Meng X., Zhang L. Application of support vector machine and genetic algorithm to network intrusion detection // 2007 International Conference on Wireless Communications, Networking and Mobile Computing. IEEE, 2007. С. 2267-2269.
4. Understanding the limits of unsupervised domain adaptation via data poisoning / Mehra A. [et al] //Advances in Neural Information Processing Systems. 2021. Т. 34. С. 17347-17359.
5. Lu S. et al. Defense against local model poisoning attacks to byzantine-robust federated learning // Frontiers of Computer Science. 2022. Т. 16. №. 6. С. 166337.
6. Гололобов Н. В., Павленко Е. Ю., Лаврова Д. С., Козачок А. В. Распознавание киберугроз на адаптивную сетевую топологию крупномасштабных систем на основе рекуррентной нейронной сети // Вопросы кибербезопасности. 2022. № 6(52). С. 93-99.
7. Orlova E. V. Methodology and models for individuals' creditworthiness management using digital footprint data and machine learning methods // Mathematics. 2021. Vol. 9. № 15.
8. An introduction to machine learning for clinicians: How can machine learning augment knowledge in geriatric oncology? / E. Ramsdale [et al.] // Journal of Geriatric Oncology. 2021.
9. Ihme M., Chung W. T., Mishra A. A. Combustion machine learning: Principles, progress and prospects: Combustion machine learning // Progress in Energy and Combustion Science. 2022. Vol. 91. P. 101010.

УДК 004.6:004.7

ВАРИАНТ ПОСТРОЕНИЯ ИЗМЕРИТЕЛЬНОЙ СЕТИ УРОВНЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА КОНТРОЛЛЕРАХ IoT

Кулешов Сергей Викторович, Аксенов Алексей Юрьевич
[1] СПИИРАН – СПб ФИЦ РАН
14 линия В. О., 39, Санкт-Петербург, 199178, Россия
e-mail: kuleshov@iias.spb.su

Аннотация. Рассматривается задача мониторинга уровня сигнала от WiFi-сетей в диапазоне 2,4 ГГц, предлагается вариант построения измерительной сети на основе контроллеров интернета вещей (IoT). Предложен вариант организации проводного сетевого взаимодействия сенсоров для сбора, передачи данных и их последующей обработки.

Ключевые слова: измерительная сеть; сбор данных; электромагнитное излучение.

METHOD FOR BUILDING A MEASURING NETWORK FOR ELECTROMAGNETIC RADIATION ON IoT CONTROLLERS

Kuleshov Sergey, Aksenov Alexey
[1] SPIIRAS – SPCRAS
39 14th Line V. I. St, Petersburg, 199178, Russia
e-mail: kuleshov@iias.spb.su

Abstract. The article discusses the problem of monitoring the signal level from WiFi networks in the 2.4 GHz range, and proposes an option for constructing a measurement network based on Internet of Things (IoT) controllers. A variant of organizing wired network interaction of sensors for collecting, transmitting data and their subsequent processing is proposed.

Keywords: sensor network; data collection; electromagnetic radiation.

В задачах оценки и мониторинга уровня электромагнитного излучения от WiFi сетей, которые не требуют метрологической точности измерений, в качестве измерительных сенсоров могут применяться WiFi контроллеры. Это может быть полезно для задач экологической безопасности, оценки защищенности помещений и т. п.

Использование программно-определяемых радиосредств для различных прикладных задач рассматривалось авторами ранее в [1, 2], данное исследование является продолжением работ в данном направлении. Измерения производятся с помощью сети датчиков S1.. S8, расположенных в точках измерений. В качестве опорного источника можно применить точку доступа (маршрутизатор) AP, в этом случае измерение будет производиться по уровню сигнала одной сети с заданным идентификатором SSID. Также возможно проведение измерений по максимальному уровню сигнала любой из доступных сетей в каждой точке измерения Si. В качестве сенсоров S1..S8 можно использовать недорогие модули ESP8266 [3], содержащие в своем составе радиомодуль WiFi и управляющий микроконтроллер с периферийными блоками и являющиеся основной для построения устройств интернета вещей (IoT). Сами радиомодули работают в пассивном режиме (STA-mode без подключения) для исключения влияния на измерение, что требует организации проводного канала связи для передачи результатов измерения на управляющий компьютер.

Канал передачи данных может быть организован на базе последовательных портов по схеме «эстафета», что позволит минимизировать количество проводников в соединительных линиях между модулями (3 провода).

Каждый сенсор Si имеет собственный уникальный числовой идентификатор (ID), определенный константой в программном коде. Программное обеспечение всех сенсоров идентично и состоит в циклическом опросе состояния радиомодуля WiFi, определение уровня сигнала RSSI требуемой сети от выбранной точки доступа AP, либо определения максимального уровня сигнала RSSI по всем доступным сетям и передачи данного значения в текстовом виде «ID:RSSI» через UART порт, а также передачи всех данных, находящихся во входном буфере UART порта дальше по цепочке модулей.

В качестве устройства сбора и последующей обработки данных измерений может использоваться ПК, подключенный по USB-порту к последнему в цепочке сенсорному модулю, получая результат конкатенации строк, содержащих результаты измерений всех модулей Si за очередной временной интервал. Так как передача данных сенсорами производится асинхронно, то для временной привязки сенсоры могут передавать инкрементируемые идентификатор номера пакета.

Предельное количество узлов определяется скоростью последовательного интерфейса для необходимой частоты опроса, и суммарной длиной соединительных кабелей между узлами, на практике может составлять несколько десятков штук.

СПИСОК ЛИТЕРАТУРЫ

1. Александров В. В., Кулешов С. В., Цветков О. В., Зайцева А. А. Концепция и теория нанотехнологии физической среды инфотелекоммуникации (прототип SDR) // Труды СПИИРАН. 2008. № 6. С. 51-57.
2. Кулешов С. В. Реконфигурируемая коммуникационная платформа передачи радиолокационных данных // Вопросы радиоэлектроники. 2010. Т. 2. № 1. С. 173-178.
3. ESP8266EX Datasheet Espressif Systems [Электронный ресурс]. URL: // https://www.espressif.com/sites/default/files/documentation/0a-esp8266ex_datasheet_en.pdf (дата обращения: 24.06.2023).

УДК 004.75: 004.056

СОЧЕТАНИЕ ПОНЯТИЙ ОТКРЫТОСТИ И БЕЗОПАСНОСТИ В ПРОТОТИПЕ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ

Нечитайленко Роман Александрович, Глущенко Артём Геннадьевич, Денисов Егор Юрьевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
e-mails: rnet2005@gmail.com, Artemglushenko98@ gmail.com, lokargenia@gmail.com

Аннотация. Сочетание понятий открытости и безопасности в прототипе распределенной системы. Распределенная система обработки информации, информационное обеспечение, открытость, безопасность системы. Рассмотрен прототип распределенной системы для поиска, обработки и анализа данных, представленный как информационно-аналитическая система, работающая в общем и распределенном пространстве данных распределенной системы, поддерживаемая сервисным и интерфейсным обслуживанием в согласованной коммуникативной форме.

Ключевые слова: распределенная система обработки информации; информационное обеспечение; открытость; безопасность системы.

THE COMBINATION OF THE CONCEPTS OF OPENNESS AND SECURITY IN THE PROTOTYPE OF A DISTRIBUTED SYSTEM

Nechitailenko Roman, Glushchenko Artem, Denisov Egor
Saint Petersburg Electrotechnical University
5 Professora Popova St, 5, St. Petersburg, 197022, Russia
e-mail: rnet2005@gmail.com, artemglushenko98@ gmail.com, lokargenia@gmail.com

Abstract. A prototype of a distributed system for data retrieval, processing and analysis is considered, presented as an information and analytical system operating in a common and distributed data space of a distributed system, supported by service and interface maintenance in a coordinated communicative form.

Keywords: distributed information processing system; information support; openness, system security.

Архитектура распределенной системы обработки информации в совокупности её функциональных, структурных, вычислительных, информационных, сервисных параметров и обеспечения, в своем прототипе представляется как информационно-аналитическая система для поиска, обработки и анализа данных, сопровожденная сервисным и интерфейсным обслуживанием в согласованной коммуникативной форме [1]. Прототип распределенной системы поддерживает основные установленные требования к распределенной системе; учитывает специфические особенности распределенной системы; информационную компоненту для поиска, обработки и анализа данных; средства управления информационным ресурсом системы; средства агрегирования и распределения данных в общем и распределенном пространстве данных распределенной системы.

В прототипе распределенной системы определены языковые, программно-технические и коммуникативные средства поддержки информационного ресурса системы; установлены правила централизованной обработки данных и рассылки / сбора данных на распределенные узлы системы; мониторинг

и фиксация информационной нагрузки по всей конфигурации распределенной системы, элементам структуры системы [2]. При выполнении целевых функций распределенной системы и планируемых предметных задач средства поддержки информационного ресурса системы поддерживают поиск, обработку и анализ данных, установленную коммуникативную форму пользователей, обращение к общим данным системы с параллельным совместным использованием ресурсов системы, но с сокрытием факта совместного использования этих ресурсов.

Разрабатываемые средств поддержки информационного обеспечения распределенной системы обработки информации сочетают качества открытости и доступности к обобщенному информационному ресурсу системы, параллельное совместное использование информационного ресурса, сокрытие различий доступа пользователей системы к предоставлению данных и средствам их специальной обработки.

Открытость и прозрачность системы в сочетании с её надежностью и безопасностью, решается как задача распределения информационной нагрузки по всей конфигурации распределенной системы и элементам её структуры [3]. Распределенная система пользователем должна восприниматься как однородный объект, наборы правил обслуживания автономных объектов, которые взаимодействуют между собой между собой, сокрыты процедурами соблюдения комплексной защиты информационного ресурса системы.

При качестве открытости распределенной системы обеспечивается возможность взаимодействия с другими открытыми системами, их информационными ресурсами, сервисными средствами сопряжения со смежными ресурсами, так что соблюдены базовые характеристики открытых распределенных систем:

– системы, входящие в состав распределенной системы и её компоненты должны легко взаимодействовать между собой;

– компоненты распределенной системы должны быть сопрягаемы с согласованными определенными интерфейсами;

– программно-техническое обеспечение распределенной системы должно обеспечивать переносимость включенных приложений;

– открытость системы достигается с помощью согласованных языков программирования, аппаратных платформ, программного обеспечения.

Прототип системы не требует адресного указания расположения необходимых ему ресурсы. Файлы данных принадлежат единому файловому пространству, могут перемещаться на различные узлы распределенной системы, обладают правилами фиксации возможных сбоев, их восстановления и отправки адресату. Одновременно обеспечивается параллельность доступа к одним и тем же данным, параллельное совместное использование общего ресурса системы, и одновременно в соответствии с правилами сокрытия обеспечивается сокрытие факта совместного использования ресурсов.

В целях обеспечения сохранности данных и соблюдения комплексной защиты информационного ресурса системы, необходимым образом обеспечивается репликация данных, при этом пользователю не будет известно, что репликация данных существует.

Безопасность адресности обращения и обработки данных всей структуры, и на уровне отдельных компонентов распределенной системы, оговаривается обеспечением совокупности оговорённых факторов безопасности:

– обеспечение аутентификации данных и ресурсов и их конфиденциальности;

– обеспечение аутентификации и ранжированния множества пользователей с обеспечением конфиденциальности доступа к ресурсам системы;

– обеспечение целостности ресурсов и данных применением политики безопасности и аутентификации пользователей.

С применением сервисных приложений распределенной системы обработки информации возможно решения задач:

– организации очередей данных в распределенных системах;

– повышения качества и скорости обработки больших данных;

– анализ свойств данных средствами централизованной обработки распределенной системы,

что допускает:

– согласовать локальные требования обработки данных компонентов распределенной системы с требованиями и задачами целостной распределенной системы;

– провести анализ свойств данных средствами централизованной обработки распределенной системы при рассылке данных на распределенные элементы структуры системы, сборе данных из распределенных элементы структуры, агрегировании данных в общее пространство данных распределенной системы;

– установить категории классификации элементов распределенных систем и их пользователей: по количеству элементов в системе, по уровню организации распределенных систем, по типу предоставляемых ресурсов, обеспечить контроль и соотношение обращений к разделам централизованного информационного ресурса системы с применением сервисных приложений распределенной системы обработки информации.

СПИСОК ЛИТЕРАТУРЫ

1. Распределенная информационно-аналитическая система для поиска, обработки и анализа пространственных данных / Шокин Ю. И. [и др.]. // Вычислительные технологии. 2007. Т. 12. Спец. Вып. 3. ГИС- и веб-технологии в междисциплинарных исследованиях. Материалы Междисциплинарной программы СО РАН 4.5.2. Вып. I. С. 108-115.
2. Steen M., Tanenbaum A. S. Distributed Systems, 4th ed., distributed-systems.net. 2023. 803 p.
3. Карабутов Н. Н. Идентификация систем. Структурный и информационный анализ. Ч. 1. М.: Изд-во Альтаир ; МГАВТ, 2005. 79 с.

УДК 004.056

МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ

Пахомов Максим Анатольевич, Соболев Николай Владиславович, Павленко Евгений Юрьевич
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: pahomov_ma@spbstu.ru, nikolay.sobolev99@mail.ru, pavlenko_eyu@spbstu.ru

Аннотация. Рассматриваются методы обеспечения информационной безопасности в беспроводных самоорганизующихся сетях, выделяются их достоинства и недостатки, выделяются группы методов, формулируются требования к методам обеспечения информационной безопасности беспроводных самоорганизующихся сетей.

Ключевые слова: информационная безопасность; беспроводные самоорганизующиеся сети; ad-hoc сети.

METHODS OF ENSURING INFORMATION SECURITY OF WIRELESS SELF-ORGANIZING NETWORKS

Pahomov Maksim, Sobolev Nikolay, Pavlenko Evgeny
Peter the Great St. Petersburg Polytechnic University,
29 Politechnicheskaya St, St. Petersburg, 195251, Russia
e-mails: pahomov_ma@spbstu.ru, nikolay.sobolev99@mail.ru, pavlenko_eyu@spbstu.ru

Abstract. Methods of ensuring information security in wireless self-organizing networks are considered, their advantages and disadvantages are highlighted, groups of methods are identified, requirements for methods of ensuring information security of wireless self-organizing networks are formulated.

Keywords: information security; wireless self-organizing networks, ad-hoc networks.

В настоящее время наблюдается активная цифровизация всех аспектов жизни человека. Появляются идеи создания инфраструктуры «умных» городов, интеллектуальных транспортных систем, промышленных и сельскохозяйственных предприятий. Большинство подобных «умных» систем используют беспроводные самоорганизующиеся сети для обмена информацией между участниками сети.

Беспроводная самоорганизующаяся сеть (ad-hoc сеть) — это сеть, не требующая централизованного управления, структура которой может динамически изменяться. В данных сетях устройство одновременно является конечным узлом и маршрутизатором. В качестве технологий передачи данных чаще всего используются Wi-Fi, WiMAX, ZigBEE, LTE [1].

Беспроводные самоорганизующиеся сети можно разделить на следующие виды:

– ячеистые сети (mesh-сети);
– мобильные самоорганизующиеся сети (MANET);
– автомобильные самоорганизующиеся сети (VANET);
– авиационные самоорганизующиеся сети (FANET);
– сенсорные сети (WSN).

Если два узла находятся в радиусе покрытия беспроводных средств связи, то они обмениваются данными напрямую, в противном случае, сообщения передаются с помощью других участников сети. В связи с этим возникает необходимость маршрутизации пакетов [2].

Маршрутизацию в беспроводных самоорганизующихся сетях можно разделить на следующие этапы:

1. Подключение узлов к сети. Инициирующий подключение узел высылает идентификационную информацию удостоверяющему центру или другим участникам сети и согласовывает протокол взаимодействия.

2. Поиск маршрутов. Участники сети осуществляют поиск соседних узлов и построение таблиц маршрутизации на основе таких показателей, как среднее потребление энергии, количество переходов до узла назначения, накладные расходы при передаче данных.

3. Передача данных. На этом этапе данные передаются от узла-источника к узлу назначения через цепочку промежуточных узлов.

4. Обслуживание маршрутов. Смысл данного этапа заключается в том, чтобы обновить таблицы маршрутизации при изменении топологии или других характеристик сети.

Как и для других типов сетей, для беспроводных самоорганизующихся сетей должна быть обеспечена информационная безопасность. Атаки на ad-hoc сети классифицируют следующим образом:

– по уровню сетевой модели TCP/IP;
– по положению нарушителя относительно сети;
– по степени воздействия на сеть;
– по этапу функционирования сети.

В ходе работы выделены следующие классы обеспечения безопасности беспроводных самоорганизующихся сетей:

– криптографические механизмы обеспечения безопасности;
– протоколы маршрутизации на основе модели доверия;

– системы обнаружения вторжений (СОВ) на основе методов машинного обучения.

Основное предназначение криптографических методов — обеспечение конфиденциальности и целостности информации, передаваемой между узлами, и идентификация узлов в сети. Поскольку ad-hoc сети децентрализованы и динамичны, одной из наибольших проблем при использовании данной группы методов является организация инфраструктуры открытых ключей. Для ее решения необходимо определить способ распределения ответственности доверенной третьей стороны между узлами.

Для распределения ответственности доверенной третьей стороны применяются пороговые схемы разделения секрета и криптографические методы на основе идентификации [3, 4].

Применение только криптографических методов не позволяет достичь высокой степени защищенности самоорганизующихся сетей от вредоносного воздействия злоумышленника. Данная группа методов не позволяет защитить сеть от атак, нацеленных на нарушение доступности информации.

Протоколы маршрутизации на основе моделей доверия в беспроводных самоорганизующихся сетях применяются на этапах поиска и обслуживания маршрутов. Их основная идея заключается в вычислении некоторым способом степени доверия к узлу, распространении этого значения всем участникам сети и исключении узлов с низкой степенью доверия из процессов маршрутизации. С их помощью возможно обеспечить доступность информации в сети [5, 6].

Однако данная группа методов требует увеличения вычислительных мощностей узлов для сбора и хранения статистической информации о трафике и поведении участников сети. Другой проблемой применения моделей доверия является сложность определения весовых коэффициентов и пороговых значений вредоносной активности. Также с помощью методов на основе моделей доверия невозможно обнаруживать атаки, нацеленные на несанкционированное чтение или модификацию информации.

СОВ на основе методов машинного обучения являются универсальным средством для обнаружения большого спектра атак. С помощью данной группы методов возможно обнаруживать атаки на всех этапах функционирования сети. Также эти методы способны обнаруживать некоторые пассивные атаки [7].

Как и другие группы методов, СОВ на основе методов машинного обучения не лишены недостатков. Для внедрения СОВ необходимо значительно расширить архитектуру сети: добавить модули сбора сетевого трафика, модули его предобработки, а также центр принятия решений. Описанные архитектурные изменения нарушают свойство децентрализованности сети и могут привести к новым угрозам информационной безопасности. Еще один значительный недостаток заключается в предназначении СОВ — эти системы применяются для обнаружения атак, а не для противодействия им. Следовательно, СОВ необходимо применять в комбинации со средствами реагирования: на основе собранного сетевого трафика СОВ выявляет вредоносные узлы, а средства реагирования исключают эти узлы из сети [8].

Использование методов только из одной группы недостаточно для обеспечения информационной безопасности беспроводных самоорганизующихся сетей. Следовательно, необходимо использовать гибридные методы, обладающие преимуществами различных групп и нивелирующие их недостатки.

Гибридный метод должен обеспечивать безопасность сети на всех этапах ее функционирования, противостоять как активным атакам нарушителя, так и пассивным.

Характеристики сетевого трафика беспроводных самоорганизующихся сетей представимы в виде временных рядов, что позволяет применять методы для их прогнозирования и выявлять вредоносное воздействие на сеть за минимальное время. Современные методы анализа временных рядов позволяют выполнять вычисления параллельно. Таким образом, вычислительная нагрузка может быть распределена между всеми участниками сети, благодаря чему сеть остается децентрализованной.

Таким образом, метод обеспечения информационной безопасности самоорганизующихся сетей должен обеспечивать безопасность на всех этапах функционирования сети, выявлять активные и пассивные атаки, сохранять свойство децентрализованности сети и учитывать ограничение вычислительных ресурсов узлов.

Финансирование: Исследование выполнено в рамках гранта Президента РФ для государственной поддержки молодых российских ученых — кандидатов наук МК-3861.2022.1.6.

СПИСОК ЛИТЕРАТУРЫ

1. Security issues in mobile ad hoc networks / Sarika S. [et al.] //Procedia Computer Science. 2016. Т. 92. С. 329-335.
2. Boulaiche M. Survey of secure routing protocols for wireless ad hoc networks // Wireless Personal Communications. 2020. Т. 114. №. 1. С. 483-517.
3. Khatoon S., Thakur B. S. Certificate less key management scheme in manet using threshold cryptography // International Journal of Network Security & Its Applications. 2015. Т. 7. №. 2. С. 55.
4. Narayana V. L., Bharathi C. R. Identity based cryptography for mobile ad hoc networks // Journal of Theoretical and Applied Information Technology. 2017. Т. 95. №. 5. С. 1173.
5. Ram Mohan C., Ananthula V. R. Reputation-based secure routing protocol in mobile ad-hoc network using Jaya Cuckoo optimization //International Journal of Modeling, Simulation, and Scientific Computing. 2019. Т. 10. №. 03. С. 1950014.
6. Arora S. K., Kumar G., Kim T. Blockchain based trust model using tendermint in vehicular adhoc networks //Applied Sciences. 2021. Т. 11. №. 5. С. 1998.
7. Legashev L., Grishina L. Development of an Intrusion Detection System Prototype in Mobile Ad Hoc Networks Based on Machine Learning Methods //2022 International Russian Automation Conference (RusAutoCon). IEEE, 2022. С. 171-175.
8. Islabudeen M., Kavitha Devi M. K. A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks //Wireless Personal Communications. 2020. Т. 112. С. 193-224.

УДК 004.056.53

КЛАСТЕРИЗАЦИЯ ДАННЫХ С ПРИМЕНЕНИЕМ НЕЙРОННОЙ СЕТИ КОХОНЕНА

Швайко Александр Сергеевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mail: sasha.shvayko2002@gmail.com

Аннотация. Рассматривается задача кластеризации, для решения которой применяется нейронная сеть Кохонена. Приводится алгоритм обучения нейронной сети. Выполняется сравнение кластеризации с другими известными методами кластеризации — *k*-ближайших соседей, логистической регрессии, случайного леса по оценке точности кластеризации.

Ключевые слова: большие данные, кластеризация, SOM-карта, гиперпараметры, обучение, точность классификации.

DATA CLUSTERIZATION USING KOHONEN NEURAL NETWORK

Shvayko Aleksander
Saint Petersburg State University of Aerospace Instrumentation
67 Bolshaya Morskaya St, St. Petersburg, 190121, Russia
e-mail: sasha.shvayko2002@gmail.com

Abstract. The problem of clustering is considered, for the solution of which the Kohonen neural network is used. An algorithm for training a neural network is presented. Clustering is compared with other well-known clustering methods — k-nearest neighbors, logistic regression, random forest to assess clustering accuracy**.**

Keywords: big data; clustering; SOM map; hyperparameters; learning; classification accuracy.

Нейронная сеть Кохонена обучается без учителя и носит название самоорганизующейся карты Кохонена. Может решать задачу кластеризации данных, а также устанавливать близость классов. Если классы изначально заданы, то сеть Кохонена может решать задачу классификации. В этой работе рассматривается применение нейронной сети Кохонена для решения задачи кластеризации, а оценка точности кластеризации проверяется на готовом датасете 4heart2.csv, содержащем записи о болезнях сердца.

Сеть Кохонена имеет всего два слоя: входной и выходной. Каждый нейрон входного слоя соединяется с каждым нейроном выходного слоя и все связи, имеют определенный вес, который корректируется в процессе обучения. Выходной слой называют также слоем топологической карты. Элементы топологической карты располагаются в некотором пространстве — как правило, двумерном. Поэтому сеть Кохонена чаще изображают в виде топологической карты, то есть только нейроны выходного слоя [1].

Обучается сеть Кохонена методом последовательных приближений. Основной итерационный алгоритм обучения сети Кохонена последовательно проходит одну за другой ряд эпох, при этом на каждой эпохе он обрабатывает каждый из обучающих примеров в следующей последовательности:

– выбрать выигравший нейрон, то есть тот, который расположен ближе всего к входному примеру;

– скорректировать выигравший нейрон так, чтобы он стал более похож на этот входной пример, вычислив квадрат евклидова расстояния между центром выигравшего нейрона и обучающего примера.

При вычислении центра нейрона-победителя используется постепенно убывающий коэффициент скорости обучения, с тем чтобы на каждой новой эпохе коррекция становилась все более тонкой. В результате положение центра установится в некоторой позиции, которая удовлетворительным образом представляет те наблюдения, для которых данный нейрон оказался выигравшим.

В результате такой итеративной процедуры обучения сеть организуется таким образом, что элементы, соответствующие центрам, расположенным близко друг от друга в пространстве входов, будут располагаться близко друг от друга и на топологической карте.

Свойство топологической упорядоченности достигается в алгоритме с помощью дополнительного использования понятия окрестности.

Окрестность — это несколько нейронов, окружающих выигравший нейрон, называется радиусом R окрестности. Подобно скорости обучения, размер окрестности убывает со временем, так что вначале к ней принадлежит довольно большое число нейронов (возможно, почти вся топологическая карта). На самых последних этапах окрестность становится нулевой, т.е. состоящей только из самого выигравшего нейрона.

Результатом такого изменения окрестностей является то, что изначально довольно большие участки сети «перетягиваются» в сторону обучающих примеров. Сеть формирует грубую структуру топологического порядка, при которой похожие наблюдения активируют группы близко лежащих нейронов на топологической карте. С каждой новой эпохой скорость обучения и радиус окрестности уменьшаются, тем самым внутри участков карты выявляются все более тонкие различия, что, в конце концов, приводит к тонкой настройке каждого нейрона.

Таким образом, в отличие от обучения с учителем, суть обучения сети Кохонена состоит не в том, чтобы сравнивать вывод сети с идеальным выводом, а в подстройке весов всех связей для максимального совпадения со входными данными.

Точность обучения нейронной сети Кохонена (*accuracy*) составила 0,88, в то время как *accuracy* для *k*-ближайших соседей — 0.77, для логистической регрессии — 0.87, для случайного леса — 0.89. Рассматриваемый метод вполне подходит для решения кластеризации и по точности соизмерим с логистической регрессией и случайным лесом. Но у нейронной сети Кохонена есть неоспоримое преимущество — визуализация кластеров в виде SOM-карты.

СПИСОК ЛИТЕРАТУРЫ

1. Пойманова Е. Д., Татарникова Т. М., Краева Е. В. Модель управления хранением трафика данных // Известия высших учебных заведений. Приборостроение. 2021. Т. 64. № 5. С. 370-375.
2. Советов Б. Я., Татарникова Т. М., Пойманова Е. Д. Модель управления масштабированием хранилища // Информационные и управляющие системы. 2020. № 5(108). С. 43-49.
3. Татарникова Т. М., Архипцев Е. Д. Определение числа реплик распределенного хранения больших данных // Международная конференция по мягким вычислениям и измерениям. 2023. Т. 1. С. 305-308.
4. Татарникова Т. М., Пойманова Е. Д. Энергетическая модель процесса хранения данных // Информация и космос. 2019. № 1. С. 89-95.

УДК 004.056

ПРИНЦИПЫ ПОСТРОЕНИЯ САМООРГАНИЗУЮЩЕЙСЯ КАРТЫ НЕЙРОСЕТИ ДЛЯ АРХИТЕКТУРЫ ЗАЩИЩЕННОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ И ИНЦИДЕНТОВ

Штеренберг Станислав Игоревич
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
Авиамоторная ул., 8а, Москва, 111024, Россия
e-mail: shterenberg.stanislaw@yandex.ru

Аннотация. Концептуальная архитектура защищенной интеллектуальной системы обнаружения вторжений и инцидентов, использует подход централизованной нейронной сети, где централизованное управление и мониторинг системы осуществляется из главного модуля под названием PiRun. Такое решение позволяет повысить контроль и обеспечивает централизованный механизм принятия решений. Но что, если на систему будет произведена атака, направленная на нарушение целостности системы? Основной идей защиты комплекса состоит в том, что после совершения атаки на нарушение целостности главный модуль системы PiRun должен принять решение на запуск самоуничтожения, программные агенты разбиться на подмодули, а сама система переключиться на децентрализованное решение.

Ключевые слова: искусственный интеллект; системы обнаружения вторжений; системы обнаружения инцидентов; нейросеть, распределённые информационные системы.

PRINCIPLES OF BUILDING A SELF-ORGANIZING NEURAL NETWORK MAP FOR THE ARCHITECTURE OF A SECURE INTELLIGENT INTRUSION AND INCIDENT DETECTION SYSTEM

Shterenberg Stanislav
Moscow technical university of communications and informatics
8a Aviamotornaya St, Moscow, 111024, Russia
e-mail: shterenberg.stanislaw@yandex.ru

Abstract. The conceptual architecture of a secure intelligent intrusion and incident detection system uses the approach of a centralized neural network, where centralized management and monitoring of the system is carried out from the main module called PiRun. This solution allows for increased control and provides a centralized decision-making mechanism. But what if an attack is made on the system aimed at violating the integrity of the system? The main idea of protecting the complex is that after committing an attack on integrity violation, the main module of the PiRun system must decide to launch self-destruction, program agents split into submodules, and the system itself switch to a decentralized solution.

Keywords: artificial intelligence; intrusion detection systems; incident detection systems; neural network, distributed information systems.

В децентрализованной интеллектуальной системе каждый компонент системы (в нашем случае программный агент) имеет свою автономность и может автономно обрабатывать, и защищать информацию без единой точки управления, что позволяет повысить безопасность и снизить риски, связанные с отказами или атаками на отдельные элементы системы. Важно отметить, что большинство из программного обеспечения чаще представлены на блок-схемах. Задача лишь состоит в том, чтобы найти составные части общего алгоритма и стабилизировать процесс глубокого обучения в дальнейшем при сборке при помощи программных агентов в правильную самоорганизующуюся карту нейронов. Ключевая технология искусственных нейронных сетей, идея которых состоит в том, чтобы максимально близко смоделировать, ну скажем, человеческий мозг, возможна, потому как стало возможным формировать ассоциативную память у интеллектуальной системы обнаружения вторжений и инцидентов в распределённой информационной системе.

Обычно, распределенной считают такую систему, в которой функционирует более одного сервера базы данных. Это применяется как для уменьшения нагрузки на сервер, так и для обеспечения работы территориально удаленных подразделений [1]. Информационные системы можно разделить на малые, средние и крупные распределенные системы по следующим факторам: сложность создания, сопровождение, модификация, взаимодействие с другими информационными системами [2].

Малые распределенные информационные системы, прежде всего использующие настольные системы управления базами данных, как правило, ориентированы на массовое использование, сложность или же невозможность изменения без участия конструкторов информационной системы, небольшой жизненный цикл, однородное аппаратно-программное обеспечение, которое не имеет средств обеспечения информационной безопасности. Алгоритм построения самоорганизующейся карты при помощи программных агентов в распределенной информационной системе следующий:

1. Поиск цели. Когда агент проникает в сеть, его первым шагом является поиск цели для распространения и эксплуатации. Агент должен понимать, где находятся нужные узлы для «заражения», и как к ним попасть. Помимо этого, агент должен отличать машины, на которые необходимо обратить внимание от машин, которые стоит пропустить;

2. Инициализация агента. После того, как агент идентифицирует цель, агент распространяет свои копии другим жертвам через различные схемы;

3. Выбор способа передачи. Передача данных агентом осуществляется через TCP и UDP. TCP-агент ориентирован на подключение и имеет ограниченную задержку. В данном случае агент блокируют выполнение потока. UDP-агент «заражается» при самостоятельном переносе. Он не имеют подключения и имеет ограниченную полосу пропускания. UDP-агент блокирует ресурсы в сети.

4. Выполнение полезной нагрузки. Под полезной нагрузкой понимается код агента. Если агент закодирован, то его труднее обнаружить в сети. Мономорфные, полиморфные и метаморфические схемы представляют собой различные форматы полезной нагрузки агента. Агент, основываясь на вышеуказанных факторах, обнаруживает цели, создает копии и выбирает средства передачи и схемы полезной нагрузки для безопасного распространения [3].

В сети существуют различные типы червей, которые вызывают задержку и ограничение пропускной способности. Некоторые из червей — это черви из списков рассылки, полиморфные черви, доброкачественные черви, черви с автозапуском, черви, проверяющие разделение и завоевание, черви, проверяющие важность, и самодисциплинарные черви [4, 5].

Данное исследование выполнено при финансовой поддержке Минцифры России (грант ИБ) в рамках научного проекта, Доп. Соглашение №. 40469-05/2022-д/1 от 22.05.2023 г.

СПИСОК ЛИТЕРАТУРЫ

1. Цехановский В. В., Чертовской В. Д. Распределенные информационные системы : учебник. 2021. С. 8-12.
2. Хабаров С. П., Шилкина М. Л. Построение распределенных систем на базе WebSocket. 2022. С. 30-32.
3. Пердиски Р., Дагон Д., Ли У., Фогла П. Вводящий в заблуждение червь. Генераторы сигнатур, использующие преднамеренное введение шума. М. : Шариф, 2006.
4. Ганапати П., Мидхунчаккараварти Д. Распространение червей в компьютерных сетях и механизмы защиты от них: обзор. 2014.
5. Пратама А., Рафрастара Ф. А. Классификация компьютерных червей // Наука и информационная безопасность. 2012. Т. 10. № 4. С. 21-24.
6. Красов А. В., Лосин Е. П, Ушаков И. А. Проблема безопасности передачи групповых рассылок в IP-сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании : сборник научных статей: в 4-х томах, Санкт-Петербург, 01–02 марта 2017 года. СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. Т. 3. С. 295-301.
7. Krasov A., Vitkova L., Pestov I. Behavioral Analysis of Resource Allocation Systems in Cloud Infrastructure // Proceedings. 2019. International Russian Automation Conference, RusAutoCon 2019, Sochi, 08–14 сентября 2019 г. Sochi : Institute of Electrical and Electronics Engineers Inc. 2019. P. 8867699.

УДК 004.932

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ МАШИННОГО ЗРЕНИЯ В УСЛОВИЯХ ОГРАНИЧЕННЫХ РЕСУРСОВ

Яковлева Екатерина Арнольдовна
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mail: y_katerina@rambler.ru

Аннотация. Рассматриваются методы машинного зрения, применяемые для распознавания объектов. Обсуждаются вопросы адаптации методов машинного зрения в условиях ограниченных ресурсов.

Ключевые слова: машинное зрение; компьютерное зрение; ограниченные ресурсы; распознавание объектов.

APPLICATION OF MACHINE VISION TECHNOLOGY IN LIMITED RESOURCE CONDITIONS

Yakovleva Ekaterina
Saint Petersburg State University of Aerospace Instrumentation
67, Bolshaya Morskaya St, St. Petersburg, 190121 Russia
e-mail: y_katerina@rambler.ru

Abstract. Computer vision methods used for object recognition are considered. Issues of adapting computer vision methods in conditions of limited resources are discussed.

Keywords: machine vision; computer vision; limited resources; object recognition.

Машинное зрение — это узконаправленные раздел компьютерного зрения, которые неразрывно связан с развитием современных информационных технологий. Использование технологий машинного зрения решает достаточно широкий круг прикладных задач. Значительный рост возможностей компьютеров, разработка новых математических методов, алгоритмов и моделей позволило расширить область применения машинного и компьютерного зрения. Задачи, имеющие практическое применение в промышленности, экономике и образовании становятся более привлекательными инвестирования [1-4].

В общем случае система машинного зрения состоит из следующих компонент:

– подсистема формирования изображений (например, объектив и ПЗС- или КМОП-матрица);

– вычислитель;

– алгоритмы анализа изображений (которые реализуются программно в процессорах, аппаратно в структуре вычислителя и/или аппаратно в подсистеме формирования изображений).

Широко используются системы машинного зрения, использующие стандартные камеры и компьютеры в качестве первых двух компонент [4]. При этом стоит отметить, что применение оптических систем не дает идеального изображения, поэтому необходима коррекция изображения. Физические характеристики оптической системы вносят существенную долю в возникновение оптических аберраций, которые устраняются на этапе постобработки специализированными программными средствами [5].

Немаловажный фактор расширения использования технологий машинного зрения — это перенос решаемых прикладных задач на миниатюрные, компактные устройства, а именно использование микрокомпьютерных и микропроцессорных систем. Минитюаризация систем машинного зрения сужает возможности их применения и снижает качество работы. Один их путей решения этой задачи — увеличение производительности микропроцессорных систем с одновременной минимизации их размеров не только ограничивает область применения. В результате, требуется разработка методов и алгоритмов машинного зрения в условиях дефицита ресурсов [6].

СПИСОК ЛИТЕРАТУРЫ

1. Горячкин Б. С., Китов М. А. Компьютерное зрение [Электронный ресурс] // E-Scio. 2020. № 9 (48). URL: https://cyberleninka.ru/article/n/kompyuternoe-zrenie-1 (дата обращения: 01.10.2023).
2. Онокой Л. С., Морев Е. А. Применение технологий компьютерного зрения в экономике и образовании // Дискуссия. 2021. № 1 (104). URL: https://cyberleninka.ru/article/n/primenenie-tehnologiy-kompyuternogo-zreniya-v-ekonomike-i-obrazovanii (дата обращения: 30.09.2023).
3. Моргунов В. В. Применение машинного зрения в области контроля качества [Электронный ресурс] // Международный студенческий научный вестник. 2019. № 2. URL: https://eduherald.ru/ru/article/view?id=19609 (дата обращения: 01.10.2023).
4. Потапов А. Системы компьютерного зрения: современные задачи и методы [Электронный ресурс] //CONTROL ENGINEERING РОССИЯ № 1 (49), 2014. типография ООО «Акцент Групп». URL: https://controleng.ru/wp-content/uploads/CE_149_sistemy_ kompyuternogo_zreniya.pdf (дата обращения: 01.10.2023).
5. Сорокин А. А., Яковлева Е. А., Коваленко Р. А. Системы трехмерного машинного зрения на микроконтроллерах и микропроцессорах : монография. Казань: Бук, 2021. 136 с.
6. Яковлева Е. А., Коваленко Р. А. Коррекция оптических искажений на примере дисторсии // Обработка, передача и защита информации в компьютерных системах 23 : Сборник докладов Третьей Международной научной конференции, Санкт-Петербург, 10–17 апреля 2023 г. СПб. : СПбГУ АЭП, 2023. С. 94-97.

УДК 007.5

ОДИН ИЗ ВАРИАНТОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ НА ЕДИНОЙ ПЛАТФОРМЕ

Янковский Никита Андреевич, Татарникова Татьяна Михайловна
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Большая Морская ул., 67, Санкт-Петербург, 190121, Россия
e-mails: yannik98@yandex.ru, tm-tatarn@yandex.ru

Аннотация. Предложена и разработана архитектура аппаратно-программного комплекса обеспечения безопасности образовательного учреждения, включающая идентификацию субъекта на базе RFID-технологии и климат-контроль в помещениях. Приведены основные компоненты, осуществляющие идентификацию и доступ в помещение на базе платформы Arduino Uno и последовательность реализации пропускного режима. Разработано необходимое программное обеспечение комплекса: веб-интерфейс для компьютера службы безопасности образовательного учреждения, база данных MySQL для хранения данных субъектов и измерений датчиков климат-контроля, способ автоматической передачи сообщений с помощью Telegram-бота.

Ключевые слова: безопасность образовательного учреждения; доступ в помещение; технология радиочастотной идентификации; климат-контроль помещения; датчики.

ONE OF THE WAYS TO ENSURE THE SECURITY OF AN EDUCATIONAL INSTITUTION ON A SINGLE PLATFORM

Yankovskii Nikita, Tatarnikova Tatiana
Saint Petersburg State University of Aerospace Instrumentation
67 Bolshaya Morskaya St, St. Petersburg, 190121 Russia
e-mails: yannik98@yandex.ru, tm-tatarn@yandex.ru

Abstract. The architecture of the hardware-software complex for ensuring the security of an educational institution was proposed and developed, including the identification of a subject based on RFID technology and indoor climate control. The main components that carry out identification and access to the premises based on the Arduino Uno platform and the sequence of access control implementation are given. The necessary software of the complex has been developed: a web interface for the computer of the security service of an educational institution, a MySQL database for storing data of subjects and measurements of climate control sensors, a method for automatically transmitting messages using a Telegram bot.

Keywords: security of an educational institution; access to the premises; RFID technology; room climate control; sensors.

В работе предлагается аппаратно-программный комплекс обеспечения безопасности образовательного учреждения на единой платформе, включающий идентификацию субъектов (сотрудников, работников и обучающихся), управление доступом в помещение, обеспечение климат-контроля и оповещение через Telegram-бот. Решение основано на технологии интернета вещей. Перспективные направлений, где интернет вещей уже активно применяется — это системы «умный дом», «умное здоровье», мониторинг окружающей среды и другие [1-4].

Разработанную систему можно рекомендовать как дополнение в системе обеспечения безопасности образовательного учреждения [5-7].

Основные компоненты, осуществляющие идентификацию и доступ в помещение:

– Arduino Uno — флагманская платформа для разработки на базе микроконтроллера ATmega328P. Для работы с платой Arduino Uno в операционной системе Windows на компьютер устанавливается интегрированная среда разработки Arduino IDE; программирование устройств Arduino основано на языке C/C++;

– Плата расширения Arduino Ethernet — для подключения Arduino Uno к глобальной сети интернет кабелем RJ-45;

– Плата NodeMCU на основе модуля (чипа) ESP8266 — для управления различными схемами на расстоянии посредством передачи сигнала в локальную сеть или интернет через Wi-Fi.

Идентификация субъекта выполняется по технологии RFID — автоматической бесконтактной идентификации по радиочастотному каналу связи [8].

Последовательность реализации пропускного режима включает следующие этапы:

– Считывание ID RFID-метки субъекта проверки;
– Передача считанного ID субъекта проверки на компьютер;
– Запрос наличия ID субъекта проверки в базе данных;
– Идентификация субъекта проверки — проверка наличия ID в базе данных;
– Вывод информации о субъекте проверки на компьютер пункта охраны;
– Передача результатов идентификации на управляемый турникет;
– Открытие доступа в случае идентификации субъекта проверки или отказ в доступе в противном случае.

Возможность передачи информации на мобильный телефон родителя, в случае установки данного комплекса в школе или колледже.

В случае установки предлагаемого решения в виде аппаратно-программного комплекса обеспечения безопасности в школе или колледже предусмотрена возможность оповещения родителей: при прохождении обучающегося через турникет, родителям, зарегистрированным в Telegram и давшим согласие на обработку персональных данных, будет приходить сообщение о том, что их ребенок зашел/вышел в/из учреждения. Для реализации данной функции создан и настроен Telegram-бот. Пользователи могут взаимодействовать с ботами при помощи сообщений, отправляемых через обычные или групповые чаты. Код для бота Telegram написан на языке программирования Python.

Для обеспечения климат-контроля в аудиториях, лабораториях, комнатах и местах общего пользования предлагается установить пироэлектрические инфракрасные (PIR) датчики движения, датчики температуры и влажности, датчики утечки газа. Этот набор практически ничем не ограничен и при необходимости может дополняться.

Последовательность реализации климат-контроля включает следующие этапы:

1. Передача данных от датчиков климат-контроля на модуль ESP8266, где выполняется предобработка и аккумуляция;

2. Передача предобработанных данных на сервер, где они сравниваются с установленными нормативными показателями и сохраняются для последующих сравнений;

3. В случае несоответствия показаний датчика установленным нормам предусмотрено срабатывание сигнализации — текстовое и звуковое сообщение.

Функции сервера выполняет компьютер на посту охраны. В качестве программного обеспечения сервера для приема запросов, их обработки и отправки ответов и системами выбран кросплатформенный веб-сервер с открытым исходным кодом Apache HTTP Server. В пользу такого выбора повлияли и другие возможности, в частности: расширяемость с помощью динамически загружаемых модулей, обработка код на большом количестве языков программирования без потребности к внешнему программному обеспечению. Благодаря веб-серверу устанавливается соединение между пользователем и сервером для обеспечения передачи данных при запросе [9, 10].

Пользователями предлагаемого аппаратно-программного комплекса являются две группы субъектов, наделенные ролью «Администратор» или ролью «Сотрудник службы безопасности».

СПИСОК ЛИТЕРАТУРЫ

1. Силакова О. В. Комплексная безопасность образовательного учреждения как важнейшее условие обеспечения безопасных условий проведения учебно-воспитательного процесса // Молодой ученый. 2014. № 18.1. С. 84-88.
2. Сенчихин С. П. Организационные проблемы обеспечения безопасности в образовательных учреждениях и пути их решения // Вопросы государственного и муниципального управления. 2022. № 2. С. 159-179.
3. Дулясова М.В., Маркин В.В. Проектное моделирование комплексноинтегрированной системы безопасности вуза // Интеграция образования. 2017. Т. 21, № 1. С. 112-123.
4. Татарникова Т. М., Богданов П. Ю., Краева Е. В. Предложения по обеспечению безопасности системы умного дома, основанные на оценке потребляемых ресурсов. Проблемы информационной безопасности. Компьютерные системы. 2020. №4. С. 88-94.
5. Татарникова Т. М., Палкин И. И. Применение парадигмы интернета вещей в концепции «умного города» // Ученые записки Российского государственного гидрометеорологического университета. 2019. № 57. С. 187-197.
6. Lee P. Internet of Things for Architects. Birmingham– Mumbai, Packt Publ. 2018. 524 p.
7. Татарникова Т. М., Елизаров М. А. Процедура разрешения коллизий в RFID-системе // Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 2. С. 150-157.
8. Bogatyrev V., Derkach A. Evaluation of a cyber-physical computing system with migration of virtual machines during continuous computing // Computers. 2020. Т. 9. № 2. С. 42.
9. Попов С. Г., Фридман В. С. Обзор методов динамического распределения данных в распределенных системах управления базами данных // Информатика, телекоммуникации и управление. 2018. Т. 11. № 4. С. 82–107.

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 378.147

СОВЕРШЕНСТВОВАНИЕ ПЕДАГОГИЧЕСКИХ МЕТОДИК ПОСРЕДСТВОМ ПРИМЕНЕНИЯ ВИРТУАЛЬНОГО ЛАБОРАТОРНОГО ПРАКТИКУМА ПРИ ИЗУЧЕНИИ КУРСАНТАМИ ОСНОВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Воронов Сергей Алексеевич, Примакин Алексей Иванович
Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: voronov-sci@mail.ru, a.primakin@mail.ru

Аннотация. Представлен опыт применения интерактивных педагогических методик и приемов в процессе изучения курсантами основных криптографических алгоритмов, используемых в прошлом и в настоящее время, с помощью авторской версии виртуального лабораторного практикума.

Ключевые слова: педагогические технологии, информационная безопасность, криптографические алгоритмы, виртуальный лабораторный практикум, методика применения виртуального лабораторного практикума.

IMPROVEMENT OF PEDAGOGICAL METHODS THROUGH THE USE OF VIRTUAL LABORATORY PRACTICE WHEN STUDYING THE BASICS OF CRYPTOGRAPHIC INFORMATION PROTECTION BY CADETS

Voronov Sergey, Primakin Alexey
St. Petersburg Military Order of Zhukov Institute of National Guard Troops of the Russian Federation
1 Pilyutov's pilot St., St. Petersburg, 198206, Russia
e-mail: voronov-sci@mail.ru, a.primakin@mail.ru

Abstract. The experience of using interactive pedagogical methods and techniques in the process of studying the main cryptographic algorithms used in the past and at present by cadets using the author's version of the virtual laboratory workshop is presented.

Keywords: pedagogical technologies, information security, cryptographic algorithms, a virtual laboratory workshop, a methodology for using a virtual laboratory workshop.

Актуальность темы связана с необходимостью разработки и внедрения новых педагогических методов и приемов к изложению учебного материала в вопросах инженерно-технической подготовки будущих офицеров Росгвардии, что продиктовано сложившимися военно-политическими условиями в мире и стране [1]. Одновременно с этим, требуется решение вопросов по обеспечению защиты информации в структурных подразделениях Росгвардии [2].

На кафедре информатики и математики Санкт-Петербургского военного ордена Жукова института войск национальной гвардии Российской Федерации курсанты изучают дисциплину «Основы информационной безопасности», тематический план которой предполагает приобретение обучающимися практических навыков по направлению криптографической защиты информации. В рамках данной учебной дисциплины курсантам необходимо освоить особенности алгоритмов шифрующих таблиц, систем шифрования Цезаря и Вижинера, «двойного квадрата» Уитстона, системы омофонов, шифра Гронсвельда, а также современные стандарты шифрования DES, RSA, ГОСТ 28147-89.

Для этого применяется разработанный преподавателями кафедры виртуальный лабораторный практикум «Контроль и обучение методам шифрования» [3]. Лабораторный практикум имеет два профиля работы: режим (профиль) обучения методам шифрования и режим проверки знаний методов шифрования.

Приступая к работе, каждый курсант на первом этапе занятия самостоятельно изучает с помощью встроенной в программу справочной системы «Помощь» или под руководством преподавателя существующие методы и алгоритмы шифрования информации, где в доступной форме представлены все необходимые криптографические алгоритмы.

Второй этап работы с лабораторным практикумом (раздел «Проверка знаний и методов шифровки») позволяет курсантам самостоятельно проверить себя — насколько правильно они поняли учебный материал.

Пройдя процедуру идентификации, курсанту предоставляется возможность с помощью ключа расшифровать то или иное сообщение, зашифрованное с помощью одного из изученных ранее криптографических алгоритмов.

Таким образом, подобный педагогический прием, построенный на интерактивной методике, лежащей в основе виртуального лабораторного практикума, повышает эффективность процесса обучения курсантов, как под руководством преподавателя, так и в часы их самостоятельной работы.

СПИСОК ЛИТЕРАТУРЫ

1. Цеханович Д. Б., Панкратов В. С. Каким быть современному военному образованию // Армейский сборник. 2022. № 12. [Электронный ресурс]. URL: http://army.ric.mil.ru/Stati/item/456129/ (дата обращения: 19.09.2023).
2. В Москве откроют центр кибербезопасности Росгвардии. [Электронный ресурс]. URL: https://www.vedomosti.ru/society/news/2021/04/27/867838-moskve-otkroyut-tsentr-kiberbezopasnosti-rosgvardii (дата обращения: 29.09.2023).
3. Примакин А. И. Практический опыт применения инновационных технологий при подготовке сотрудников в области обеспечения защиты информации правоохранительных органов // Информационные технологии, связь и защита информации МВД России. 2012. Вып. 2. 2012. С. 90-92.

УДК 377.112.4

ПОДГОТОВКА БУДУЩИХ КАДРОВ ПО УПРАВЛЕНИЮ БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ

Грачев Александр Михайлович
Государственное бюджетное общеобразовательное учреждение школа № 219
Красносельского района Санкт-Петербурга
Маршала Казакова ул.,68, Санкт-Петербург, 198335, Россия
e-mail: gam1404@mail.ru

Аннотация. В работе предлагается внедрить в программу подготовки учеников старших классов проведение занятий по авиационному моделированию и практических занятий по развитию навыков управления беспилотными летательными аппаратами.

Ключевые слова: развитие навыков; беспилотные летательные аппараты; авиационное моделирование; программа подготовки.

TRAINING FOR FUTURE MANAGEMENT STAFF UNMANNED AERIAL VEHICLES

Grachev Alexander
State budgetary educational institution school No. 219 Krasnoselsky district of St. Petersburg
68 Marshal Kazakov St, St. Petersburg, 198335, Russia
e-mail: gam1404@mail.ru

Abstract. The paper proposes to introduce into the training program for high school students the conduct of classes in aviation modeling and practical exercises to develop skills in controlling unmanned aerial vehicles.

Keywords: skills development; unmanned aerial vehicles; aviation modeling; training program.

Развитие современности происходит настолько быстро, что становится необходимостью быть образованным во всех сферах деятельности человека и общества. Подготовка школьников старших классов по программе авиационного моделирования и управлении беспилотными летательных аппаратами (БЛА, БПЛА) всё больше становится необходимой.

В настоящее время просматривается быстрое развитие БПЛА, в связи с этим данное направление становится актуальным. Вопросы в необходимости получения навыков управления БПЛА рассматривался следующими авторами: А. В. Сафонова, А. Р. Котков, О. Л. Сафонов [1], В. Н. Ромашин [2], Т. В. Ларина, И. И. Кораблин [3] и другие. Данные авторы рассматривают необходимость повышения профессиональной культуры в подготовке специалистов беспилотной авиации как можно раньше.

Для развития навыков, умений и навыков по управлению БЛА предлагается внедрить в школьную программу теоретическую часть по авиационному моделированию и обязательную практическую часть по развитию навыков управления БПЛА. Решение данного вопроса на школьном этапе позволит ученикам старших классов получить практические навыки и быть подготовленными в направлении пилотирования БПЛА. Внедрение программы может быть осуществлено и как внеурочная деятельность, что позволит рассмотреть на первоначальном этапе интерес к этой программе обучающихся.

Таким образом, внедрение в школьную учебную программу старшеклассников программ по БЛА позволит повысить кругозор, развить навыки, умения и навыки, а также приобрести важный опыт в управлении ими и возможно, как следствие повлияет на выбор будущей профессии.

СПИСОК ЛИТЕРАТУРЫ

1. Сафонова А. В., Котков А. Р., Сафонов О. Л. Особенности подготовки профессиональных кадров по использованию навигационной системы беспилотных летательных аппаратов в военном вузе // Проблемы и современные пути развития образования в области аэронавигации : Сборник материалов V Всероссийской педагогической научно-методической конференции, Сызрань, 24 мая 2020 г. С. : Межрегиональный центр инновационных технологий в образовании, 2020. С. 106-109. EDN EJTPTC.

2. Ромашин В. Н. Требования, предъявляемые к офицерским кадрам, и пути повышения качества военно-профессиональной подготовки курсантов // Омский научный вестник. О., 2009. № 1(75). С. 133-137. EDN MVLGDV.
3. Ларина Т. В., Кораблин И. И. Сущность и специфика профессиональной культуры будущих военных специалистов беспилотной авиации // Мир науки, культуры, образования. 2018. № 6(73). С. 67-69. EDN YUJMTJ.

УДК 004 056.5

БОРЬБА С УГРОЗАМИ В СОЦИАЛЬНЫХ СЕТЯХ

Кононов Олег Александрович, Кононова Ольга Васильевна
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Большая Морская ул., 67, Санкт-Петербург, 190000, Россия
e-mail: o2kon@mail.ru

Аннотация. В докладе рассмотрены актуальные вопросы информационной безопасности при использовании социальных сетей.

Ключевые слова: социальные сети; информационно-коммуникационные технологии; информационная безопасность, киберстрахование, система образования.

FIGHTING THREATS IN SOCIAL NETWORKS

Kononov Oleg, Kononova Olga
Saint-Petersburg State University of Aerospace Instrumentation,
67 Bolshaya Morskaya St, St. Petersburg,190000, Russia,
e-mail: o2kon@mail.ru

Abstract. The report deals with topical issues of information security when using social networks.

Keywords: social networks; information and communication technologies; information security, cyber insurance, education system.

Социальные сети в настоящее время для многих являются основным местом проведения времени в Интернете и позволяют совершенно незнакомым людям найти общий язык, как посредством общения, так и посредством открытой информации, которую оставляют пользователи. Например, для улучшения взаимодействия чиновников РФ с аудиторией органы власти обязаны вести аккаунты в таких социальных сетях, как «Одноклассники» и «Вконтакте», согласно распоряжению правительства с 1 декабря 2022 года [1]. Речь, в частности, идет о публикации сведений о своей работе, отчетов о мероприятиях, комментариев по актуальным вопросам, контактной информации, включая адрес электронной почты и номера телефонов.

COVID-19 ускорил распространение социальных сетей, при этом увеличение времени пребывания в соцсетях произошло на фоне сокращения общего количества времени, которое люди проводят онлайн. В январе 2023 года в Российской Федерации насчитывалось 106,0 миллионов пользователей социальных сетей [2].

В то же время, согласно [3] за год блокировки к февралю 2023 года аудитория ранее популярных соцсетей Instagram и Facebook упала соответственно в 5 раз и в 3,5 раза. Эти сети принадлежат компании Meta, которая была признана экстремистской и запрещена на территории России. Соответственно среднесуточный охват соцсетей Telegram и «ВКонтакте» в феврале 2023 года вырос к аналогичному месяцу предыдущего года почти в 1,8 раза — с 23 до 41 %. У «ВКонтакте» этот показатель увеличился в 1,15 раза — до 44 %, а у «Одноклассников» в 1,12 раза — до 18 % [3].

Очевидно, что на динамику среднесуточного охвата пользователей соцсетей и мессенджеров в России будет влиять процесс формирования общественного спроса на безопасные технологии.

Действительно, обращение к ресурсам социальных сетей не всегда является безопасным.

Во-первых, могут быть похищены персональные данные, например, через анализ предпочтений пользователей с целью предоставления услуг, которые могут быть использованы в корыстных целях. Во-вторых, возможна кража учетных записей пользователей социальных сетей, не уделяющих должного внимания вопросам информационной безопасности. В-третьих, к сожалению, сама архитектура сети Интернет оставляет возможность осуществления перехвата или изменения информации, передаваемой через сеть, в том числе и конфиденциальной. Вместе с тем существует сложность определения местоположения и личности самого преступника, который может перенаправлять данные на другие сервера, используя VPN-технологии и технологии перераспределения логических и физических адресов.

В снижении уровня киберугроз в РФ заинтересованы все участники информационного взаимодействия и, как следствие, должны принимать активное участие в создании и внедрении безопасных технологий.

Так на государственном уровне 31.07.2023 года принят Федеральный закон № 408-ФЗ «О внесении изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации», согласно которому владельцы сайтов и сервисов, на которых производится анализ предпочтений пользователей РФ с целью предоставления услуг, обязаны [4]:

– не допускать предоставление такой информации на основе метрик с нарушением прав граждан или законодательства РФ;

– предупреждать пользователя сервиса, сайта или ПО о наличии таких технологий, применяющих метрики. Не допускается предоставление информации на основе метрик без такого предупреждения;

– регламентировать применение таких технологий, анализирующих метрики, и разместить разработанную политику в общем доступе на ресурсах, где такие технологии применяются;

– разместить адрес электронной почты на ресурсах, где применяются такие технологии, для получения юридических значимых сообщений.

Политика использования технологий анализа предпочтений [4]:

– должна иметь описание процессов и методов сбора, систематизации, анализа сведений, относящихся к предпочтениям пользователей Интернета, предоставления информации на основе этих сведений, а также способов осуществления таких процессов и методов;

– должна описывать виды сведений, относящихся к предпочтениям пользователей Интернета, которые используются для предоставления информации с применением рекомендательных технологий, источники получения таких сведений;

– быть общедоступна и бесплатна для просмотра;

– должна быть составлена на русском языке.

Нарушения требований федерального закона № 408-ФЗ:

в случае нарушения данных требований, Роскомнадзор имеет право проводить разбирательства по факту обнаружения нарушений, в т.ч. запрашивать доступ к системе обработки метрик для проведения собственного исследования. Владелец ресурса обязан в течение 10 дней предоставить ответ на запрос или запрошенный доступ, по факту обнаружения нарушений, Роскомнадзор имеет право направить требования по устранению замечаний. При получении такого требования, владелец обязан в течение суток прекратить предоставление информации на основе системы анализа метрик (но не информации в целом) и устранить замечания в течение 10 дней, если иное не будет указано в требованиях,если владелец ресурса не останавливает предоставление информации с использованием системы анализа метрик (т.е. продолжает предоставлять услуги, используя механизмы анализа предпочтений), то Роскомнадзор имеет право направить требование к оператору связи о полном блокировании доступа к ресурсу. Оператор связи обязан выполнить такое требование и ограничить доступ к ресурсу, например, по сети Интернет (т.е. полностью его заблокировать).

В конце июля 2023 года был также опубликован Федеральный закон от 31.07.2023 № 401-ФЗ с поправками в КоАП. С 1 сентября 2023 года соцсети, нарушающие запреты на размещение нежелательного, вредного или опасного для общества контента, будут штрафовать [5].

На уровне бизнес-сообщества представляется целесообразным инвестировать не только в инструменты превентивной кибербезопасности, позволяющие снизить степень успешности кибератак, но и иметь план на случай инцидента, включая полис киберстрахования, который обеспечит наилучшее покрытие.

Общий объем страховых премий по киберстрахованию в России за 2022 г., по оценке Всероссийского союза страховщиков, составляет около 750 млн рублей [6]. Объем премий по киберстрахованию вырастет в ближайшие два года в три раза, а по итогам 2023 года составит 1350 млн рублей. В будущем рынок страхования киберрисков в России может вырасти до 10 млрд рублей. Если на данный момент, на этот вид страхования приходится менее 1 % от всех сборов в корпоративном сегменте рынка, то через несколько лет его доля, в силу развития и популяризации IT-решений, станет существенно более значимой.

На уровне общества существенный вклад в решение задачи внедрения в сознание участников информационного взаимодействия необходимости соблюдения правовых и этических норм поведения в социальных сетях и привития навыков их применения может и должна внести система образования.

Разъяснение и пропаганду этих норм необходимо проводить в рамках теоретических дисциплин и практических занятий, формируя, таким образом, общественное мнение. Обучающиеся должны понимать основные правовые, социальные и этические аспекты обеспечения информационной безопасности общества. Они должны сознавать свою личную роль в этом процессе. Социально-личностное развитие обучаемых по различным специальностям, как техническим, так и сугубо гуманитарным, имеет чрезвычайно важное значение для обеспечения информационной безопасности общества [7].

Информационно-коммуникационные технологии при их умелом использовании могут и должны стать мощным инновационным ресурсом совершенствования промышленности, науки и образования. При этом социальные сети могут служить инструментом развития, однако необходимо учитывать таящиеся в них опасности.

СПИСОК ЛИТЕРАТУРЫ

1. Правительство обязало органы власти вести аккаунты в соцсетях [Электронный ресурс]. URL: https://lenta.ru/news/2022/09/05/soccc/(дата обращения 19.08.2023).
2. Статистика интернета и соцсетей на 2023 год — цифры и тренды в мире и в России [Электронный ресурс].URL: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-i-v-rossii/ (дата обращения 18.08.2023).
3. За год блокировки аудитория Instagram упала в 5 раз, а Facebook — в 3,5 раза [Электронный ресурс].. URL: https://www.vedomosti.ru/media/articles/2023/03/04/965272-auditoriya-instagram-upala (дата обращения 19.08.2023).
4. Федеральный закон от 31.07.2023 № 408-ФЗ »О внесении изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. URL: https://rtmtech.ru/news/fz-408/ (дата обращения 19.08.2023).
5. Федеральный закон от 31.07.2023 № 401-ФЗ »О внесении изменений в Кодекс Российской Федерации об административных правонарушениях». URL: http://publication.pravo.gov.ru/document/0001202307310014 (дата обращения 19.08.2023).
6. ВСС: По итогам 2023 года рынок киберстрахования составит 1,35 млрд рублей. URL: https://consult-cct.ru/vss-po-itogam-2023-goda-rynok-kiberstrahovaniya-sostavit-135-mlrd-rublej (дата обращения 19.08.2023).
7. Кононов О. А. Кононова О. В. Гуманитарные аспекты информационной безопасности и система образования. Информационная безопасность регионов России (ИБРР-2021). XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 27-29 октября 2021 г.: Материалы конференции СПб. : СПОИСУ, 2021. С. 369-371.

УДК 004.05, 004.5

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ ПРОЦЕССОМ ПРОВЕДЕНИЯ КЛИНИЧЕСКОЙ ПРАКТИКИ СТУДЕНТАМИ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Сафронова Мария Вадимовна, Ныркoв Анатолий Павлович
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: maryaeihteen@gmail.com, kaf.koib@gmail.com

Аннотация. В данной статье описываются этапы проектирования и разработки системы автоматизации процессов прохождения студентами клинической практики, а также выбранные программные меры защиты от компьютерных атак.

Ключевые слова: автоматизированная система управления; проектирование; разработка; обучение IT-специалистов.

AUTOMATED CONTROL SYSTEM FOR THE PROCESS OF CONDUCTING STUDENTS CLINICAL PRACTICE IN PROTECTED VERSION

Safronova Marya, Nyrkov Anatoliy
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: maryaeihteen@gmail.com, kaf.koib@gmail.com

Abstract. This article describes the stages of designing and developing a system for automating the processes of passing clinical practice by students, as well as the selected software measures to protect against computer attacks.

Keywords: automated control system; design; development; training of IT specialists.

Практики, обеспечивающие формирование общепрофессиональных компетенций, определяемых ФГОС ВО, входят в обязательную часть программы бакалавров и специалистов, а обеспечивающие формирование профессиональных компетенций определяются вузом самостоятельно [1]. В Государственном университете морского и речного флота имени адмирала С. О. Макарова было принято решение проводить практики для ИТ направлений в подразделениях Управления информатизации университета.

При большом количестве обучающихся встаёт вопрос об автоматизации процесса прохождения обучающимися практики. Было решено разработать автоматизированную систему, которая сможет упростить процесс прохождения клинической практики студентами. Такая система позволяет хранить большие объемы данных, отслеживать процесс выполнения заданий, предлагать задачи исполнителям в зависимости от уже имеющихся у них навыков, а также обмениваться сообщениями с наставниками, контролирующими процесс выполнения заданий, в реальном времени и создавать отчеты об успеваемости исполнителей.

Система представляет собой web-приложение, так как данная технология проста в реализации и удобна в использовании для большого количества пользователей, не требует установки отдельных программ и средств защиты для каждого клиента, доступ к системе может быть реализован посредством обычного браузера [2].

Проектирование системы велось средствами языка UML, была построена диаграмма вариантов использования системы, описывающая функционал разрабатываемой программной системы доступный каждой группе пользователей. Были выделены 6 групп пользователей, которые могут взаимодействовать с системой: Администратор, Управляющий, Заказчик, Исполнитель, Наставник, Неавторизованный пользователь.

Для более детального описания особенностей функционального поведения системы был разработан шаблон сценариев, описывающий действия пользователей и поведение моделируемой системы в форме обычного текста. Для каждого варианта использования в шаблоне сценариев представлен свой раздел, описывающий ход событий выполнения данного варианта использования и исключительные ситуации, которые могут возникнуть [3].

При разработке системы использовалась модель MVC, аббревиатура которой расшифровывается как «модель-представление-контроллер». Это способ организации кода, который предполагает выделение блоков, отвечающих за решение разных задач.

Данная модель повышает безопасность приложения за счет:

– Разделение обязанностей между компонентами модели. Это облегчает управление и контроль над каждой составляющей приложения.
– Централизованной проверки пользовательского ввода.
– Упрощение тестирования [4].
– Для разработки модулей системы были выбраны следующие средства разработки:
– Для проектирования базы данных была выбрана технология PostgreSQL.

Для разработки серверной части приложения был выбран язык PHP, распространённый язык программирования общего назначения с открытым исходным кодом, специально сконструированный для веб-разработок и его код может внедряться непосредственно в HTML.

JavaScript — мультипарадигменный язык программирования. Поддерживает объектно-ориентированный, императивный и функциональный стили.

Centrifugo — масштабируемый сервер обмена сообщениями в реальном времени [5].

При разработке модулей были учтены российские и мировые стандарты по безопасности, такие как OWASP Top 10, CAPEC (Common Attack Pattern Enumeration and Classification), CWE (Common Weakness Enumeration), CVE (Common Vulnerabilities and Exposures), Банк данных угроз безопасности информации ФСТЭК России, Mitre *Att&ck*, STIX (Structured Threat Information eXpression), WASC (Web Application Security Consortium), модель Kill Chain [6]. Для системы были разработаны следующие модули:

Модуль «База данных» — совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ [7]. Спроектированная база данных хранит информацию о пользователях системы, правах пользователей, выполняемых задачах, сообщениях пользователей, методических материалах для обучения.

Модуль «Администрирование». Разработка модуля Администрирование включила в себя разработку инструментов «Заказчики», «Исполнители» и «Наставники», а также инструментов «Заявки», «Планировщик» и «Взаимодействие».

Разработка модуля «Чат» включает в себя создание модуля для быстрого обмена сообщениями между исполнителями и наставниками, методов для записи и получения сообщений из базы данных. Для получения сообщений в реальном времени используется протокол WebSocket (протокол связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером, используя постоянное соединение). Соединения посредством web-сокетов реализуется на сервере Centrifugo.

Для Безопасной интеграции модуля базы данных в систему были выбраны следующие средства:

Каждый сервис в системе разворачивать на отдельной docker контейнере, что повышает безопасность за счет изоляции частей системы и ограничения привилегий контейнера по умолчанию.

Для связи базы данных и серверной части используется библиотека PDO (PHP Data Objects) — это универсальный интерфейс для работы с базами данных в PHP, поддерживающий подготовленные запросы, которые защищают приложение от SQL-инъекций.

Модуль «Чат» расположен в защищенной части web-приложения, доступ к которой имеют только авторизованные пользователи. Для того, чтобы пользователи получали сообщения в реальном времени они подключаются к серверу Centrifugo. Когда пользователь заходит на страницу чата, сервер генерирует ключи доступа пользователя к приватным каналам. Таким образом, пользователь может получать сообщения только из тех чатов, в которых он состоит.

Были реализованы программные меры защиты от типовых атак на web-приложение:

- защита от угроз нарушения контроля доступа;
- защита от SQL injection;
- защита от XSS атак;
- защита от CSRF атак;
- регистрация и мониторинг событий в системе;
- настройка безопасности на сервере;
- защита от криптографических сбоев;
- защита от брутфорс атак.

Проведена проверка разработанных модулей на безопасность сканером уязвимостей OWASP ZAP. OWASP (Open Web Application Security Project) — всемирная некоммерческая организация, деятельность которой направлена на повышение безопасности ПО. OWASP ZAP — это один из самых популярных в мире инструментов безопасности с открытым исходным кодом. В результате сканирования: не найдены уязвимости, которые могут навредить системе, но найдена информация об используемых компонентах веб-сайта. Это можно исправить дополнительными настройками безопасности на сервере.

На данный момент разработанная автоматизированная система введена в тестовую эксплуатацию. Программную систему можно использовать для автоматизации процессов прохождения клинической практики студентами. Система обеспечивает непрерывный процесс получения практических навыков обучающимися, а также отслеживания их успеваемости. Представленные алгоритмы предотвращения компьютерных атак разрабатывались с учётом Российских и мировых стандартов по безопасности. Дальнейшие исследования будут связаны с повышением безопасности разработанной системы. Также система предоставляет потенциал для дальнейшего развития и внедрения новых функций и возможностей.

СПИСОК ЛИТЕРАТУРЫ

1. О формировании профессиональных компетенций обучающихся по направлению «Информационная безопасность» в транспортных вузах / Ныркова А. П. [и др.]. // Информационная безопасность регионов России (ИБРР–2019). XI Санкт–Петербургская межрегиональная конференция : Материалы конференции. СПб. : СПОИСУ, 2019. С. 523-524.
2. Ильина А. А., Шипунов И. С. Мобильное приложение для организации учебного процесса студента // Актуальные аспекты и приоритетные направления развития транспортной отрасли. СПб., 2019. С. 172-176.
3. Буч Г., Рамбо Д., Якобсон И. Введение в UML от создателей языка. 2017.496 с.
4. Архитектурный паттерн MVC. Веб-платформа. [Электронный ресурс]. URL: https://doka.guide/tools/architecture-mvc/ (дата обращения: 07.08.2023).
5. Centrifugo introduction. CENTRIFUGO. Scalable real-time messaging server. Set up once and forever. [Электронный ресурс]. URL : https://centrifugal.dev/ (дата обращения: 07.08.2023).
6. Общий обзор классификаций угроз безопасности: OWASP, CWE, CAPEC, WASC. Безопасность пользователей в сети Интернет. [Электронный ресурс]. URL : https://safe-surf.ru/specialists/article/5210/595970/ (дата обращения: 07.08.2023).
7. Ныркова А. П., Ныркова А. А. Сравнительная оценка математического обеспечения систем управления базами данных // Сборник научных трудов Задачи контроля и управления. СПб : СПГУВК, 1997. С. 142–145.

УДК 004.658.6

РАЗРАБОТКА ЦИФРОВОЙ БИРЖИ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ РЕЗУЛЬТАТОВ ПГУПС

Соломатова Мария Феликсовна, Смелов Илья Максимович,
Доцаев Тимур Артурович, Пак Владислав Павлович
Петербургский государственный университет путей сообщения Императора Александра I
Московский пр., 9, Санкт-Петербург, 190031, Россия
e-mails: isaeva@pgups.ru, smeloff62@gmail.com, dotsaev_timur@bk.ru, vladikpark2002@gmail.com

Аннотация. Данная статья рассматривает проблему отсутствия единой системы хранения и обмена научными результатами в Петербургском государственном университете путей сообщения Императора Александра I. Основной предмет и тема работы заключаются в необходимости создания цифровой биржи для сбора и централизованного хранения научных данных, с целью обеспечения доступности для всех пользователей, включая исследователей, преподавателей и студентов.

Ключевые слова; Разработка; цифровая биржа научно-исследовательских результатов; цифровые технологии, базы данных; система управления.

DEVELOPMENT OF A DIGITAL EXCHANGE OF RESEARCH RESULTS

Solomatova Maria, Smelov Ilya, Dotsaev Timur, Pak Vladislav
Emperor Alexander I St. Petersburg State Transport University
9 Moscow Av, St. Petersburg, 190031, Russia
e-mails: isaeva@pgups.ru, smeloff62@gmail.com, dotsaev_timur@bk.ru, vladikpark2002@gmail.com

Abstract. This article addresses the problem of the lack of a unified system for storing and exchanging research results at the Imperial Alexander I St. Petersburg State Transport University. The main subject and theme of the work involve the necessity of creating a digital exchange for the collection and centralized storage of scientific data to ensure accessibility for all users, including researchers, teachers, and students.

Keywords: Development; digital exchange for research results; digital technologies.

В Петербургском государственном университете путей сообщения Императора Александра I отсутствует единая система для хранения и обмена научно-исследовательскими результатами. Это усложняет доступ к информации как среди внешних исследователей, так и среди сотрудников и студентов Университета. Для устранения этой проблемы необходимо создать цифровую биржу [1, 2], которая позволит собирать и хранить все научные данные в одном месте и обеспечивать доступность для всех пользователей. Этот проект направлен на оптимизацию процессов в области научных исследований внутри университетской среды.

Главная цель проекта – обеспечить создание и внедрение цифровой биржи, предоставляющей исследователям, преподавателям и студентам возможность хранения, обмена и поиска научных результатов. Этот сайт будет предоставлять единое и удобное пространство для хранения и обмена данными, объединяя научные исследования как университетского персонала, так и студентов. Проект стремится устранить отсутствие системы, способной централизованно хранить и предоставлять доступ к результатам научных исследований в университете. Данная работа выполняется при поддержке Федеральным государственным бюджетным образовательным учреждением высшего образования «Петербургский государственный университет путей сообщения Императора Александра I» инициативных научных работ, выполняемых студенческими научными коллективами.

Цифровая биржа необходима университету, так как она позволит собирать и хранить все научно-исследовательские результаты, достигнутые сотрудниками и обучающимися в одном месте и обеспечит их постоянную доступность для всех желающих.

Реализация данного проекта включает в себя несколько ключевых этапов. Необходимо разработать требования к функциональности и дизайну сайта, изучить существующие инструменты для создания электронных каталогов [1], подготовить и структурировать материалы, отражающие основные научные исследования университета.

Проект предоставляет новизну, так как электронные каталоги в научно-исследовательской сфере не так распространены, и обычно используются обычные архивы без категоризации. Реализация цифровой биржи будет представлена в виде веб-приложения, что обеспечит интерактивность и кроссплатформенность, а также облегчит доступ к электронному каталогу [2-3].

Результатом проекта считается полностью разработанный и готовый к внедрению цифровой каталог, разработанный с использованием технологий PostgeSQL [4] и React-Bootstrap [5], обеспечивающий удобство использования с различных устройств, включая мобильные.

Одним из ключевых аспектов проекта является его потенциал для коммерциализации. Пользователи смогут бесплатно пользоваться платформой, получая доступ через официальный сайт университета. Это позволит усилить привлекательность университета и укрепить связи с научным сообществом.

Таким образом, научно-исследовательская деятельность, ориентированная на создание и внедрение цифровой биржи научных исследований, имеет важное значение для университета и научного сообщества в

целом. Проект предоставляет решение для организации хранения, доступа и обмена научными результатами, а также обладает потенциалом внедрения в различных областях, включая образование и производство.

СПИСОК ЛИТЕРАТУРЫ

1. Методические рекомендации по разработке репозиториев [электронный ресурс]. М.: Ваше цифровое издательство, 2018. 34 с. URL: https://openrepository.ru/images/docs/Metod_Schwarzman.pdf (дата обращения: 24.06.2023).
2. Ковязина Е. В. Открытый архив в научном центре: особенности формирования // Распределенные информационно-вычислительные ресурсы. Наука – цифровой экономике (DICR-2017). Труды XVI всероссийской конференции. Институт вычислительных технологий СО РАН. 2017. С. 434-440. URL: http://elib.ict.nsc.ru/jspui/bitstream/ICT/1467/115/paper56.pdf (дата обращения: 24.06.2023).
3. Горбунов Д.В. Концептуальная модель и принципы создания биржи инновационных проектов // УЭкС. 2015. №4 (76). URL:https://cyberleninka.ru/article/n/kontseptualnaya-model-i-printsipy-sozdaniya-birzhi-innovatsionnyh-proektov (дата обращения: 10.09.2023).
4. PostgreSQL: Documentation: 14: PostgreSQL 14.8 Documentation [электронный ресурс]. URL: https://www.postgresql.org/docs/14/index.html (дата обращения: 10.09.2023).
5. React-Bootstrap React-Bootstrap Documentation [электронный ресурс]. URL: https://react-bootstrap.github.io/ (дата обращения: 10.09.2023).

УДК 004.451:004.056

ИЗУЧЕНИЕ МЕХАНИЗМОВ ИЗОЛЯЦИИ РЕСУРСОВ ОПЕРАЦИОННОЙ СИСТЕМЫ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО «КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

Частухин Даниил Алексеевич, Широков Владимир Владимирович, Щиголева Марина Андреевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197022, Россия
e-mails: dudypool@yandex.ru, vvshirokov@mail.ru, vvcehanovsky@mail.ru

Аннотация. Рассматриваются вопросы изучения механизмов пространства имен «контрольные группы» в дисциплинах обучения по направлению «Компьютерная безопасность». Данный механизм позволяет изолировать ресурсы дочерних процессов от ресурсов процессов-родителей. Такая изоляция позволяет существенно повысить безопасность выполнения процессов в среде операционной системы. Возможно использование при подготовке по направлению «Информационные системы и технологии».

Ключевые слова: операционная система; программный интерфейс операционной системы; компьютерная безопасность; изоляция ресурсов; пространства имен процессов; контрольные группы.

STUDYING THE MECHANISMS OF ISOLATION OF OPERATING SYSTEM RESOURCES DURING THE TRAINING OF SPECIALISTS IN «COMPUTER SECURITY»

Chastuhin Daniil, Shirokov Vladimir, Schigoleva Marina
Saint Petersburg Electrotechnical University
5 Professor Popov St, St. Petersburg, 197022, Russia
e-mail: dudypool@yandex.ru, vvshirokov@mail.ru, vvcehanovsky@mail.ru

Abstract. The issues of studying the mechanisms of the name space «control groups» in the discipline in the areas of «Computer security» are considered. This mechanism allows you to isolate the resources of child processes from the resources of parent processes. Such isolation can significantly increase the security of process execution in the operating system environment. It can be used in training in the direction of «Information systems and technologies».

Keywords: operating system; operating system software interface; computer security; resource isolation; process namespaces; control groups.

Пространства имен в операционных системах предоставляют механизмы изоляции ресурсов дочерних процессов от ресурсов родительских процессов. Эти механизмы лежат в основе построения таких важнейших и широко распространенных средств обеспечения информационной безопасности компьютерных систем, как контейнеры [1].

Дисциплины профессиональной подготовки по направлениям обучения «Компьютерная безопасность» и «Информационные системы и технологии» преподаются в концепции обеспечения компьютерной безопасности всех этапов реализации информационных технологий отраслевых и специализированных информационных систем широкого профиля назначения. При использовании стандартных и разрабатываемых операционных сред изначально должна быть предусмотрена необходимость обеспечения безопасность выполнения процессов в среде операционной системы. Во всех вопросах проектирования, разработки, управления, интерфейсного обеспечения, задача сохранения компьютерной безопасности должна опираться на предлагаемые программно-технические решения. Освоение приёмов ограничения доступа и изоляции возможных несанкционированных утечек информационного ресурса, наработанное в ходе обучения как обязательный подход предотвращения нарушения безопасности, позволяет подготовить специалистов, для которых атрибут компьютерной и информационной безопасности будет неотъемлемой составляющей всех принимаемых предпроектных решений.

В профильной подготовке специалистов в области информационных систем и технологий необходимо делать акцент на то, что то или иное решение поддерживает информационную и компьютерную безопасность разрабатываемой или применяемой информационной технологии и информационной системы. Для примера, в дисциплинах по изучению применяемых операционных систем, необходимо подчеркнуть, какими процедурами

обеспечения безопасности обладает операционная система, какие средства её реализации позволяют расширить функциональные возможности операционной системы и какие атрибуты компьютерной безопасности при этом надо предусмотреть. Так в дисциплине «Операционные системы» можно показать механизмы ограничения доступа к информационному ресурсу операционной системы. Одним из таких механизмов является механизм пространств имен. Данный механизм позволяет изолировать ресурсы дочерних процессов от ресурсов процессов-родителей и существенно повысить безопасность выполнения процессов в среде операционной системы.

Разработана методика, позволяющая наглядно показать, как шаг за шагом решается задача обеспечения безопасности обращения к операционному ресурсу, с использованием понятий пространства имён, дочерних процессов, ресурсов процессов-родителей, процесса-потомка, процесса-родителя, механизмы функционирования контейнеров. Методика позволит изолировать ресурсы дочерних процессов от ресурсов процессов-родителей.

Подготовлена методика изучения и проверки возможностей управления ресурсами процессов на основе контрольных групп и изоляции ресурсов с помощью механизма пространства имен Cgroup.

Пространство имен Cgroup, для которого установка соответствующего флага (CLONE_NEWCGROUP) должна продемонстрировать отсутствие «видимости» процессами определенных ветвей файловой системы. В этом случае процесс-потомок «не видит» ветку дерева файловой системы в каталоге /sys/fs/cgroup, описывающую контрольную группу процесса-родителя. Такая изоляция не позволяет процессу-потомку воздействовать на ресурсы процесса-родителя.

На первом этапе изучения механизма контрольных групп у предлагается создать контрольную группу по определенному виду ресурсов. Наиболее наглядным для этой цели является ресурс памяти. Для этой цели необходимо создать каталог в файловой системе /sys/fs/cgroup/memory, например, /sys/fs/cgroup/memory/test_cgroup. При создании каталога /sys/fs/cgroup/memory/test_cgroup в нем автоматически создается группа файлов, содержащих информацию о контрольной группе. Например, в файле cgroup.procs будут содержаться идентификаторы процессов, принадлежащих этой группе, а в файле memory.limit_in_bytes будет содержаться ограничение на объем памяти, которым могут пользоваться процессы, принадлежащие этой группе. При создании файла memory.limit_in_bytesв нем записаны данные, говорящие об отсутствии ограничений на размер памяти.

Включить процесс в контрольную группу можно, записав его идентификатор (pid) в файл cgroup.procs, а ограничить размер памяти процессам группы можно, записав этот размер в файл memory.limit_in_bytes.

Проверку изучаемых механизмов можно производить одним из двух способов. Первый — это с помощью команд операционной системы в терминале. Второй — с помощью программирования, используя программные интерфейсы.

Для этого необходимо предварительно ознакомиться с программными интерфейсами создания дочерних процессов с возможностью создания новой контрольной группы [2]. К таким интерфейсам относится функция clone(), в набор параметров которой могут входить перечисленные выше флаги типов пространств имен, в том числе и CLONE_NEWCGROUP. Другим видом интерфейса является совместное использование функций fork() и unshare(). То есть создаваемый функцией fork() дочерний процесс должен вызвать функцию unshare() с передачей флага типа пространства имен, и тем самым продолжить свое выполнение в новом, изолированном от процесса-родителя пространстве.

Как сказано в документации [3], «когда процесс создает новое пространство имен контрольной группы с помощью clone() или unshare() с флагом CLONE_NEWCGROUP, его текущие cgroups каталоги становятся корневым cgroup каталогом нового пространства имен».

Вариантом проверки видимости каталогов cgroups в процессе-потомке: использование в процессе-потомке вызова функции system(«/bin/bash»). В этом случае процесс-потомок вызывает внутри себя командный интерпретатор. В нем необходимо с клавиатуры выдать команду «cd /proc/self» для перехода в каталоге /proc в подкаталог процесса-потомка /proc/[pid]. Затем выдать команду «cat cgroup», чтобы вывести на экран содержимое файла cgroup. Этот файл содержит путь в файловой системе /sys/fs/cgroup к подкаталогу, описывающему контрольную группу, в которую входит процесс-потомок. Затем необходимо выдать команду «exit», чтобы из командного интерпретатора вернуться в процесс-потомок.

Поскольку вызов функции system() не является предпочтительным в программах, которые требуют привилегий, а вызовы clone() и unshared() с флагом CLONE_NEWCGROUP требуют привилегий администратора (CAP_SYS_ADMIN). Поэтому для наблюдения за содержимым файла /proc/[pid]/cgroup целесообразно прямое открытие файла вызовом fopen() с последующим чтением содержимого функцией fread() и закрытием функцией fclose().

Если процесс-потомок выполняется в общем с процессом-родителем пространстве Cgroup, то через содержимое файла /proc/[pid]/cgroup ему доступен весь путь к каталогу, описывающему контрольную группу процесса-родителя, вплоть до каталога /sys/fs/cgroup. Это позволяет процессу-потомку воздействовать на ограничение ресурсов процесса-родителя вследствие ошибочных или умышленных действий.

Если процесс-потомок выполняется в изолированном от процесса-родителя пространстве Cgroup, то содержимое файла /proc/[pid]/cgroup — это корневой каталог. То есть процесс-потомок не может подняться по дереву файловой системы к ограничениям ресурсов процесса-родителя и, соответственно, не имеет возможности воздействовать на них.

При изучении механизмов пространства имен контрольных групп методика позволяет самостоятельно получить результаты, подобные представленным, и выполнить анализ полученных результатов с точки зрения возможного воздействия процесса-потомка на ресурсы процесса-родителя. Самостоятельное прохождение по алгоритму выполнения, наглядность выполнения отдельных этапов методики, последовательная подводка к логичному обоснованному выводу, позволит лучше понять внутренние механизмы функционирования контейнеров, одним из элементов построения которых являются пространства имен.

СПИСОК ЛИТЕРАТУРЫ

1. Райс Л. Безопасность контейнеров. Фундаментальный подход к защите контейнеризированных приложений. СПб.: Питер, 2021. 224 с.
2. Широков В. В., Щиголева М. А. Методические рекомендации по практическому освоению программных интерфейсов пространств имен операционных систем // Современное программирование. III Всероссийская научно-практическая конференция. Нижневартовск, 26-27 ноября 2020. С. 295-299.
3. Cgroup_namespaces [Электронный ресурс] // Обзор пространств имен cgroup в Linux: Описание. Обзор пространств имен. URL: https://man7.org/linux/man-pages/man7/cgroup_namespaces.7.html (дата обращения 16.03.2023).

УДК 004.056.5 (371.693.4)
ГРНТИ 81.93.29

ВИРТУАЛЬНЫЙ ТРЕНАЖЕР КАК СПОСОБ ОБУЧЕНИЯ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Шейхов Глеб Вагифович, Липатников Валерий Алексеевич, Островский Юрий Николаевич, Васильев Никита Алексеевич, Ледовская Кристина Геннадьевна
Военная академия связи им. С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: gleb.sheyhov@yandex.ru, vasn2020@mail.ru

Аннотация. Виртуальный тренажер, разработанный для обучения будущих специалистов в сфере проведения специального обследования объектов информатизации, необходим в связи с высокой стоимостью оборудования, требуемого для физического обучения выделенных помещений, и потребностью в снижении затрат и повышении качества обучения.

Ключевые слова: информационная безопасность; специальное обследование; виртуальная реальность; виртуальные тренажеры, объекты информатизации

VIRTUAL SIMULATOR AS A WAY OF TRAINING FUTURE SPECIALISTS IN TECHNICAL PROTECTION OF INFORMATION

Sheikhov Gleb, Lipatnikov Valery, Ostrovsky Yuri, Vasiliev Nikita, Ledovskaya Kristina
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S. M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: gleb.sheyhov@yandex.ru, vasn2020@mail.ru

Abstract. A virtual simulator designed to train future specialists in the field of conducting a special survey of informatization objects is necessary due to the high cost of equipment required for physical training in allocated rooms, and the need to reduce costs and improve the quality of training.

Keywords: information security; special examination; virtual reality; virtual simulators, informatization objects

Развитие информационных технологий привело к появлению новых возможностей для людей, однако также создало новые вызовы в области обеспечения безопасности информационных систем. В настоящее время обеспечение безопасности таких систем является критически важным аспектом для защиты Российской Федерации. Иностранные разведывательные службы современными технологиями активно пытаются перехватывать информацию с информационных систем, чтобы получать разнообразные данные, включая секретную информацию.

Исследования в области информационных систем показывают, что в последние годы активно разрабатывается новая современная технология — технология обеспечения безопасности информации в компьютерных системах и сетях передачи данных. Однако для продвижения и развития этой технологии требуются значительные финансовые вложения. Несмотря на это, такие инвестиции помогают предотвращать серьезные потери и ущерб, которые могли бы возникнуть из-за угроз информационным системам и технологиям.

Основная цель этой разработки заключается в улучшении практической подготовки специалистов путем включения обучающихся в исследование данной области с помощью визуализационных технологий и взаимодействия с виртуальным тренажером для обнаружения скрытых устройств. Это позволяет сократить затраты на специальное оборудование, благодаря использованию стереоскопической визуализации модели тренажера.

Для достижения этой цели был разработан алгоритм, который обеспечивает эффективное взаимодействие с виртуальным тренажером. Виртуальный тренажер создает специализированную среду для обучения в определенном помещении, позволяя тренироваться без необходимости использования специальных устройств. В нем присутствуют виртуальные инструменты для обнаружения различных типов скрытых устройств.

Также в работе представлены рекомендации по обнаружению скрытых устройств с применением организационно-технических мер, которые в определенной степени помогают решить эту проблему. В рамках исследования был составлен обширный список технических средств для поиска электронных устройств, которые были классифицированы и изучены в отношении их технических характеристик и особенностей работы. Также были представлены рекомендации по использованию этих средств в практической деятельности органов, ответственных за защиту информации, и проведению специальных работ по методике специального обследования.

Применение виртуального тренажера в учебном процессе позволяет проводить практические занятия по специальному обследованию без необходимости покупки дорогостоящего специализированного оборудования.

СПИСОК ЛИТЕРАТУРЫ

1. Островский Ю. Н., Васильев Н. А. Используя цифровые технологии виртуальный тренажёр по развёртыванию аппаратной связи // Вестник военного образования : журнал. 2022. № 4 (37). С. 83-86.
2. Линовес Д. Виртуальная реальность в Unity. ДМК Пресс, 2016. 313 с.
3. Безопасность информационных систем : учеб. пособие. М.: Флинта ; Наука, 2015. 184 с.
4. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами : учеб. пособие. СПб. : НИУ ИТМО. 2012. 416 с.
5. Жук И. Е. Концептуальные основы информационной безопасности // Информация и безопасность. 2010.
6. Пахомова А. С., Пахомов А. П., Разинкин К. А. К вопросу о разработке структурной модели угрозы компьютерной разведки // Информация и безопасность. 2013.
7. Чаплыгина М. П. Методика контроля защищенности автоматизированной системы обработки конфиденциальной информации от несанкционированного доступа к информации // Молодой ученый. 2016. С. 169.
8. Костарев С. В., Карганов В. В., Липатников В. А. Технологии защиты информации в условиях кибернетического противоборства : науч. монография / Под общ. ред. В. А. Липатникова. СПб. : ВАС, 2020. 716 с.
9. Липатников В. А., Тихонов В. А. Распознавание вторжений нарушителя при управлении кибербезопасностью инфраструктуры интегрированной организации на основе нейронечетких сетей и когнитивного моделирования // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019) : сб. науч. статей VIII Международной научно-технической и научно-методической конференции : в 4 т. 2019. С. 659–664.
10. Липатников В. А., Ломанов А. А. Способ обнаружения и классификации многоэтапной атаки на основе долгой краткосрочной памяти // Технологии. Инновации. Связь : сб. материалов научно-практической конференции. СПб., 2022. С. 104-108.
11. Lipatnikov V. A., Kuzin P. I., Rabin A. V. The method of increasing the reliability of noise immunity when receiving information in radio communication systems of the SHF and EHF ranges // Journal of Physics: Conference Series. Krasnoyarsk, Russian Federation, 2020. P. 52100.
12. Rabin A. V., Lipatnikov V. A., Kuzin P. I. Signal protection methods in channels with Nakagami fading // JOP Conference Series: Metrological Support of Innovative Technologies. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. K., 2020. С. 52078.
13. Тренажерно-обучающие системы с применением технологий виртуальной и дополненной реальности / А. И Осадчий. [и др.] // Информация и космос. 2021. № 1. С. 65-72.
14. Островский Ю. Н., Шайсултанов М. Х. Нейрокомпьютерный интерфейс для обучающих систем военного назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. научных статей. В 4-х т. 2018. С. 520-524.

УДК 004.5,004.58

ПРОЕКТ «ИТ КЛИНИКИ» В ГУМРФ ИМЕНИ АДМИРАЛА С. О. МАКАРОВА»

Шипунов Илья Сергеевич, Ныркov Анатолий Павлович, Шипунова Диана Алексеевна
Государственный университет морского и речного флота имени адмирала С. О. Макарова
Двинская ул.,5/7, Санкт-Петербург, 198035, Россия
e-mails: shipunovis@gumrf.ru, kaf.koib@gmail.com, shipunovada@gumrf.ru

Аннотация. Рассматриваются предпосылки создания ИТ клиники в ГУМРФ имени адмирала С. О. Макарова, ее цели и задачи. Определен круг бенефициаров. Обоснована необходимость создания АИС для управления работой ИТ клиники в защищенном исполнении.

Ключевые слова: морской ВУЗ; ИТ; ИТ клиника; клиническая практика; образование; АИС.

THE PROJECT «IT CLINICS» IN ADMIRAL MAKAROV SUMIS

Shipunov Ilya, Nyrkov Anatoliy, Shipunova Diana
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: shipunovis@gumrf.ru, kaf.koib@gmail.com, shipunovada@gumrf.ru

Abstract. The prerequisites for the establishment of the IT Clinic at Admiral Makarov State University of Maritime and Inland Shipping, its goals and objectives are considered. The circle of beneficiaries is defined. The need to create an AIS for managing IT clinic in a secure design is substantiated.

Keywords: Maritime University; IT; IT clinic; clinical practice; education; AIS.

В 2017 году в Российской Федерации была сформирована и утверждена национальная программа «Цифровая экономика Российской Федерации» (далее — Программа). Программой определены цели, задачи, направления и сроки реализации основных мер государственной политики по созданию необходимых условий для развития в России цифровой экономики, в которой данные в цифровом виде являются ключевым фактором

производства во всех сферах социально-экономической деятельности, что является необходимым условием повышения конкурентоспособности страны, качества жизни граждан, обеспечения экономического роста и национального суверенитета [1].

Для управления программой определены пять базовых направлений развития цифровой экономики в России на период до 2024 года. К базовым направлениям отнесены: нормативное регулирование, кадры и образование, формирование исследовательских компетенций и технических заделов, информационная инфраструктура и информационная безопасность.

Важным аспектом реализации данной программы являются специалисты в сфере ИТ, которых готовят современные вузы. Развитие подходов к подготовке ИТ кадров сегодня задает тональность развитию и остальных направлений подготовки. Важной частью обучения на сегодняшний день является получение практических навыков [2-5]. Одной из новых форм в данной сфере образования является прохождение практики на базе ИТ клиники, созданной университетом.

Клиническая практика — это форма получения практических навыков без отрыва от учебного процесса для решения задач, поставленных клиентом (сотрудником университета, преподавателем).

В Государственном университете морского и речного флота имени адмирала С. О. Макарова ИТ клиника была запущена в сентябре 2022 года. Цели и задачи ИТ клиники:

– повышение уровня компетенций обучающихся в области ИТ [6, 7];
– прохождение практики на базе ГУМРФ обучающимся по информационным направлениям подготовки;
– подготовка выпускников к решению современных задач в области цифровизации и цифровой трансформации [8];
– обучение командной работе над практическими задачами в области ИТ [9-11];
– реализация идей цифровизации ГУМРФ при опытной поддержке специалистов управления информатизации и преподавателей [12-14];
– проведение на базе клиники тематических хакатонов, проведение полноценных стартап-конкурсов, летних тематических школ и дополнительных образовательных программ.

В круг бенефициаров входят: более 1200 обучающихся по образовательным программам направлений ИТ; более 700 преподавателей, нуждающихся в ИТ поддержке; подразделения ГУМРФ; партнёры ГУМРФ, потенциальные работодатели (подготовка кадрового резерва для ИТ компаний, открытие центров компетенций, для не ИТ компаний — решение ИТ задач на базе Университета).

В ходе работы клиники в первый месяц стало очевидно, что для эффективного управления данным подразделением необходимо создать Автоматизированную информационную систему — АИС «ИТ клиника». Это обусловлено огромным количеством участников клиники при управляющем составе из двух человек — делопроизводителя и руководителя. Важным аспектом при создании АИС «ИТ клиника» стало применение методов и моделей проектирования защищенных информационных систем [15, 16].

Клиническая практика — это важный элемент обучения новых кадров, полностью соответствующий программе «Цифровая экономика Российской Федерации». Это значит, что данный подход к подготовке кадров будет только набирать обороты, а разработки различных информационных систем только подстегнут этот процесс. Стоит отметить, что наряду с ИТ клиникой в Государственном университете морского и речного флота имени адмирала С.О. Макарова уже инициирована Юридическая клиника, а также запущенны в разработку на ранней стадии Экономическая клиника (центр финансовой грамотности), строительная клиника и лингвистическая клиника. Автоматизированная система, о которой идет речь в данной статье, может быть применена и в этих подразделениях, а работы по доработке имеющихся в разработке новых необходимых инструментов может взять на себя ИТ клиника.

СПИСОК ЛИТЕРАТУРЫ

1. Цифровая экономика РФ [Электронный ресурс] URL: https://digital.gov.ru/ru/activity/directions/858/?utm_referrer=https%3a%2f%2fwww.google.com%2f/ (дата обращения: 07.08.2023).
2. Кардакова М. В., Ныркова А. П., Цымай Ю. В. Концепция игрового тренажера по информационной безопасности на речном транспорте // Речной транспорт (XXI век). М., 2022. № 3 (103). 2022. С. 45–49.
3. Kardakova M. V., Nyrkov A. P., Tsymay Y. V. Water Transport Information Security Trainer Concept (final part) // XIII International Conference on Transport Infrastructure: Territory Development and Sustainability (TITDS-XIII 2022). Volume 68. Transportation Research Procedia 68. 2023. Pp. 372–382. https://doi.org/10.1016/j.trpro.2023.02.050.
4. Shipunov I., Nyrkov A., Korotkov V., Alimov O., Knysh T. Principles of using modern IT trends in maritime shipping // E3S Web Conf., 203 (2020) 05005. Published online: 2020-11-05 DOI: https://doi.org/10.1051/e3sconf/202020305005.
5. Ныркова А. П., Алексеев С. А., Стахно Р. Е. Структурно-функциональная модель обучающегося в системе тренажерной подготовки по судовождению // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. 2018. Т. 10. № 6. С. 1288-1298. https://doi.org/10.21821/2309-5180-2018-10-6-1288-1298.
6. Ныркова А. П., Каторин Ю. Ф., Ныркова А. А., Белов А. В. О формировании профессиональных компетенций обучающихся по направлению «Информационная безопасность» в транспортных вузах // «Информационная безопасность регионов России (ИБРР–2019)» XI Санкт–Петербургская межрегиональная конференция. Материалы конференции. СПб. : СПОИСУ, 2019. С. 523–524.
7. Ныркова А.П., Каторин Ю. Ф., Ныркова А. А. Естественно-научные дисциплины в формировании профессиональных компетенций обучающихся по направлению «Информационная безопасность» в транспортных вузах // Тезисы докладов национальной научно-практической конференции профессорско-преподавательского состава ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова». СПб : Изд-во ГУМРФ им. адм. С.О. Макарова, 2019. С. 153-154.
8. Антохина Ю. А., Ныркова А. П., Варжапетян А. Г. Риски образовательной деятельности в современных рыночных условиях // «Экономика и управление». 2012. № 8. С. 35-41.

9. Подготовка кадров в области обеспечения информационной безопасности в условиях совершенствования системы качества образования в высшей школе / А. В. Алексеев [и др.] // Труды конференции «Информационная безопасность регионов России (ИБРР–2007). V Санкт–Петербургская межрегиональная конференция». СПб.: СПОИСУ, 2008. С. 218-220.
10. Нырков А. П. Проблемы подготовки кадров в области информационной безопасности и прохождение лицензионной экспертизы специальности // «Научно–методические и нормативные материалы и документы XII пленума УМО по образованию в области информационной безопасности». Т. : «В–Спектр», 2008. С. 199-202.
11. Алексеев А. В., Нырков А. П., Степанов С. А. Подготовка и переподготовка кадров в области обеспечения информационной безопасности в условиях совершенствования системы качества образования в высшей школе // Материалы конференции «V Санкт–Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР–2007)». СПб.: СПОИСУ, 2007. С. 127-128.
12. Теплов Э. П., Гатчин Ю. А., Нырков А. П., Сухостат В. В. Гуманитарные аспекты информационной безопасности: методология и методика поиска истины, построения доказательства и защиты от манипуляций. СПб. : Университет ИТМО, 2016. 120 с.
13. Гуманитарные аспекты информационной безопасности: основные понятия, логические основы и операции / Теплов Э. П. [и др.]. СПб. : Университет ИТМО, 2016. 122 с.
14. Теплов Э.П., Нырков А. П., Башмаков А. В., Брагина Е. К. Гуманитарные аспекты информационной безопасности: получение, анализ и оценка деловой информации. СПб. : Издательский Дом «Афина», 2016. 160 с.
15. Методы обеспечения информационной защищенности данных электронной информационно-образовательной среды университета / Соколов С. С. [и др.]. // «Региональная информатика и информационная безопасность» : сб. трудов. СПб.: СПОИСУ, 2017. Вып. 4. С. 309–312.
16. Нырков А. П., Соколов С. С., Башмаков А. В. Методика проектирования безопасных информационных систем на транспорте // Проблемы информационной безопасности. Компьютерные системы. СПб., 2010. № 3. С. 58-61.

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «ЭКОСИСТЕМА БЕЗОПАСНЫХ ГОРОДСКИХ ЦИФРОВЫХ СЕРВИСОВ»

УДК 323.213

ОБЗОР ПОДХОДОВ К ОЦЕНКЕ ЦИФРОВЫХ СЕРВИСОВ

Аркатов Дмитрий Александрович[1,2]
[1]Высшая школа экономики
Грибоедова канала наб., 123, Санкт-Петербург, 190068, Россия
[2]Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
email: darkatov@hse.ru

Аннотация. Существует значительное количество рабочих рамок для оценки цифровых сервисов правительства. В данной работе анализируется основные из них и предлагается для использования наиболее комплексная «сбалансированная рейтинговая доска».

Ключевые слова: цифровые сервисы; электронное правительство; оценка цифровых сервисов.

DIGITAL SERVICES EVALUATION FRAMEWORKS: A REVIEW

Arkatov Dmitriy [1,2]
[1] High School of Economics
123 Griboedova canal Emb, St. Petersburg, 190068, Russia
[2] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
email: darkatov@hse.ru

Abstract. There are numerous frameworks in literature which are aimed at evaluating e-government performance. In this paper the most common frameworks are discussed and the most developed framework created by Tambouris et al. is suggested for practical usage.

Keywords: digital services; e-government; evaluation framework.

Органы государственной власти во многих странах и городах все чаще обращаются к созданию так называемых «коллаборативных» инструментов планирования и осуществления политики, аргументируя это тем, что такой подход повышает качество управления [1, 2]. Для оценки цифровизации государственного управления было создано значительное количество рабочих рамок, направленных на рейтингование различных аспектов электронного правительства и его сервисов. Данные рамки используют различные метрики и индексы, а также методологические подходы, что связано с тем, что успех функционирования таких инициатив связан с широким спектром политических, экономических, технологических и инфраструктурных факторов.

Подходы к оценке цифровых сервисов правительств зависят от исследовательских и прикладных областей, из которых они происходят. Модели оценки из проектного менеджмента включают такие подходы как: а) оценка жизненного цикла программного обеспечения б) модели готовности проекта по стандартам проектного менеджмента и в) «базы знаний» по внедрению отдельных проектов. Прикладные модели оценки цифровых сервисов чаще всего представлены исследованиями и метриками международных организаций, таких как ООН, Всемирный банк, Главного директората по коммуникационным сетям ЕС, а также различных консалтинговых компаний.

Среди комплексных исследовательских рамок наиболее ключевой, предопределившей развитие последующих подходов стала модель успеха информационных систем ДеЛона — МакЛина [3]. В ее основе лежит 6-блоковая структура, направлена на оценку технического уровня реализации систем и предоставляемой информации, уровня ее использования и качество пользовательского опыта, а также индивидуального и организационного эффекта от внедрения определенной системы. Постулируется, что в данном случае нет определенной «зависимой переменной» и все эти элементы взаимосвязаны.

На основе данной модели была разработана «сбалансированная рейтинговая доска», которая является наиболее комплексной и позволяет оценить организационную, техническую, информационную перспективы, а также социально-экономические показатели и удовлетворенность граждан [4, p. 85]. Сюда включаются такие индексы как прямые и непрямые расходы, обучение сотрудников, доступность сервисов и пользовательский опыт. Последний подразумевает рейтингование удовлетворенности граждан, и надежности сервисов.

Исследование выполнено за счет гранта Российского научного фонда и Санкт-Петербургского научного фонда № 23-18-20079 «Исследование социальной результативности электронного взаимодействия граждан и власти в Санкт-Петербурге на примере городских цифровых сервисов» (https://rscf.ru/project/23-18-20079/).

СПИСОК ЛИТЕРАТУРЫ

1. Santamaria-Philco A., Canos Cerda J. H., Penades Gramaje M. C. Advances in e-Participation: A perspective of Last Years // IEEE Access. 2019.
2. Newig, J., Challies, E., Jager, N.W., Kochskaemper, E. and Adzersen, A. The Environmental Performance of Participatory and Collaborative Governance: A Framework of Causal Mechanisms // Policy Studies Journal. 2018. № 2 (46). P. 269–297
3. Iivari J. An empirical test of the DeLone-McLean model of information system success // ACM SIGMIS Database: the DATABASE for Advances in Information Systems. 2005. № 2 (36). С. 8–27
4. Tambouris E., Liotas N., Tarabanis K. A Framework for Assessing eParticipation Projects and Tools Waikoloa, HI, USA: IEEE, 2007.C. 69–90.

УДК 316.354

ПРОНИКНОВЕНИЕ ЦИФРОВЫХ МЕДИЦИНСКИХ СЕРВИСОВ В СРЕДУ ПОЖИЛЫХ ЖИТЕЛЕЙ ПЕТЕРБУРГА

Видясова Людмила Александровна[1,2], Толстикова Ирина Ивановна[1,2]
[1]СИ РАН — филиал ФНИСЦ РАН,
7-я Красноармейская, д. 25/14, Санкт-Петербург, 190005, Россия
[2] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: bershadskaya.lyudmila@gmail.com, tolstikova_irina@mail.ru

Аннотация. Рассматриваются результаты исследования проникновения цифровых медицинских сервисов в среду пожилых жителей Петербурга. Исследование проведено методом анкетирования 210 пожилых в медицинском учреждении. По результатам опроса сделаны выводы об использовании информационных технологий людьми старшей возрастной группы.

Ключевые слова: пожилые; цифровые сервисы; медицинские сервисы; Интернет-проникновение.

PENETRATION OF DIGITAL MEDICAL SERVICES INTO THE ENVIRONMENT OF ELDERLY RESIDENTS OF PETERSBURG

Vidiasova Lyudmila[1,2], Tolstikova Irina[1,2]
[1] SI RAS - branch of the FNISC RAS,
7th Krasnoarmeyskaya, 25/14, St. Petersburg, 190005, Russia
[2] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: bershadskaya.lyudmila@gmail.com, tolstikova_irina@mail.ru

Abstract. The results of a study of the penetration of digital medical services into the environment of elderly residents of St. Petersburg are considered. The study was conducted by the method of questioning 210 elderly people in a medical institution. Based on the results of the survey, conclusions were drawn about the use of information technologies by people of the older age group.

Keywords: elderly; digital services; medical services; Internet penetration.

В последние десятилетия повсеместное проникновение цифровых технологий открывает новые модели общения и взаимодействия, но также обостряет определенные барьеры и проблемы, к которым относится цифровое неравенство [1]. За последние десятилетия социальный статус и место пожилых в обществе существенно поменялись [2].

В докладе представлены результаты исследования, проведенного в мае-июне 2023 г. для выявления проникновения цифровых сервисов в среду пожилых жителей Петербурга. Исследование проведено методом очного анкетирования в ФГБУ СЗОНКЦ им. Л.Г. Соколова ФМБА России. В опросе приняли участие 210 респондентов в возрасте от 60 лет до 91 года, преимущественно женщины. Исследование проводилось по методике, разработанной и апробированной в 2022 г. [3]. По результатам исследования, среди опрошенных людей старшего возраста 17 % считают себя опытными пользователями Интернета и компьютера и легко осваивают новые программы. Примерно 10% регулярно используют Интернет для взаимодействия с органами власти. Доверяют онлайн взаимодействию с властью через Интернет 12% опрошенных.

В исследовании отдельный блок вопросов был посвящен проникновению цифровых сервисов здравоохранения. По данным опроса, 56% пользовались порталом Госуслуги, 38% сервисом «Мое здоровье» на портале Госуслуги, 33% порталом «Здоровье Петербуржца», 23% заводили личные кабинеты в медицинских учреждениях, 47% записывались к врачу через Интернет, 50% получали данные анализов и исследований в электронном виде, 25% пользовались электронной медицинской картой, 16%- телемедицинскими консультациями, 24% оставляли обратную связь о медицинском обслуживании, 20% пользуются приложениями мониторинга здоровья, 15% — фитнес-приложениями. Важно отметить, что по сравнению с данными опроса, проведенного в 2022 году, был заметен рост почти в 2 раза проникновения сервисов портала «Здоровье петербуржца» и сервиса «Мое здоровье» на портале Госуслуги.

Таким образом, полученные результаты говорят об увеличении проникновения цифровых медицинских сервисов в среду пожилых жителей Петербурга.

Исследование выполнено за счет гранта Российского научного фонда № 22-18-00461 «Отложенное старение или поздняя взрослость в России: как цифровое развитие меняет статус пожилых в эпоху COVID-19 и неопределенности» (https://rscf.ru/project/22-18-00461/).

СПИСОК ЛИТЕРАТУРЫ

1. Aissaoui N. The digital divide: a literature review and some directions for future research in light of COVID-19 // Global Knowledge, Memory and Communication. 2022. Vol. 71 (8/9). P. 686-708.
2. Boudiny K. Active ageing: From empty rhetoric to effective policy tool // Ageing society. 2023. Vol. 33 (6). P. 1077–1098.
3. Видясова Л.А., Кузнецова Е.М., Григорьева И.А. Интеграция пожилых людей в информационное пространство: исследовательский кейс Санкт-Петербурга // Успехи геронтологии. 2022. Т. 35, № 5. С. 668-678.

УДК 316.776 304.3

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ГОСУДАРСТВЕННЫХ СЕРВИСОВ КАК ФАКТОР СОЦИАЛЬНОГО САМОЧУВСТВИЯ: НА ПРИМЕРЕ САНКТ-ПЕТЕРБУРГА

Видясова Людмила Александровна, Якубова Мария Юрьевна
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: bershadskaya.lyudmila@gmail.com, shentorin@gmail.com

Аннотация. Статья представляет собой результаты социологического исследования, который выявил связь между цифровыми сервисами и благополучием жителей Санкт-Петербурга. Онлайн-опрос 500 жителей города показал, что на социальное самочувствие влияют такие факторы, как уверенность в ИТ-навыках, удобство сервисов, доверие к онлайн взаимодействию с властью и эффективность сервисов. Планируется разработка методики оценки благополучия с учетом данных из социальных медиа и других открытых источников.

Ключевые слова: цифровые сервисы; государственные электронные сервисы; социальное самочувствие; опрос; ИТ-навыки; экосистема городских сервисов.

THE USE OF DIGITAL PUBLIC SERVICES AS A FACTOR OF SOCIAL WELL-BEING: THE EXAMPLE OF ST. PETERSBURG

Vidiasova Lyudmila, Yakubova Maria
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: bershadskaya.lyudmila@gmail.com, shentorin@gmail.com

Abstract. The article presents the results of a sociological study that revealed a connection between digital services and the well-being of residents of St. Petersburg. An online survey of 500 city residents showed that factors such as confidence in IT skills, convenience of services, trust in online interactions with authorities, and service efficiency influence social well-being. The development of a methodology for assessing well-being is planned, including data from social media and other open sources.

Keywords: digital services; public electronic services; social well-being; survey, IT skills; urban services ecosystem.

В последние годы становится актуальным поиск факторов, способствующих формированию социальной устойчивости в регионе. В данной статье представлены результаты комплексного социологического исследования, касающегося запросов к цифровым сервисам среди жителей Петербурга, а также влияния удовлетворенности от использования этих сервисов на уровень социального благополучия.

Влияние Интернета на поведение людей и их социальное самочувствие представляет большой интерес для исследователей [1]. Анализ литературы показывает, что «социальное самочувствие» — понятие довольно размытое, но позволяющее оценить уровень удовлетворенности некоторых потребностей в обществе. Отечественные исследования выделяют такие параметры социального самочувствия, как уровень защищенности, удовлетворенность жизнью и социальный оптимизм [2]. Зарубежные исследования выделяют личное «счастье», благополучие и такие компоненты, как экономическая стабильность, семейные отношения и качество окружающей среды. Социальное самочувствие оказывается связанным с социальными связями, субъективным благополучием и перспективами будущего у пенсионеров [3].

В апреле 2022 года был проведен онлайн-опрос среди петербуржцев старше 18 лет. Анкета опроса была основана на методике измерения использования цифровых сервисов и доверия к ним [4]. Анкета оценивала такие показатели, как: актуальность сервисов, частота использования электронных каналов для контакта с органами власти и организациями, степень применения цифровых каналов для разных задач, опыт работы с цифровыми технологиями, доверие к институтам и технологиям, опыт использования цифровых сервисов, оценка взаимодействия между гражданами и представителями власти в режиме онлайн.

Для оценки социального состояния использовали методологию ВЦИОМ, с вопросами о материальном положении, удовлетворенности жизнью, взглядах на экономический кризис и ожиданиях на будущее [5].

Исследование проводилось на основе поставленной гипотезы о взаимосвязи между использованием цифровых сервисов и уровне социального самочувствия населения. Население Санкт-Петербурга было разделено на 5 возрастных групп (18–30, 31–40, 41–50, 51–64, 65+), для расчета были использованы данные Петростата о численности населения.

Опрос проводился через онлайн сервис Анкетолог, с базой в 14 тыс. зарегистрированных петербуржцев. Выборка составила 500 человек (доверительная вероятность 95%). Респондентам, удовлетворяющим условиям выборки, были разосланы приглашения принять участие в опросе. Время заполнения анкеты составило около 11 минут, отклик — 85 %.

Участники опроса: 72 % с высшим, 21 % со средним специальным и 7 % с неполным средним образованием. По сферам занятости: служащие/специалисты — 41 %, неработающие пенсионеры — 22 %, рабочие/водители — 10 %, руководители — 8 %, бизнесмены — 4 %, учащиеся/студенты — 4 %, домохозяйки — 4 %, временно не работающие — 4 %, другие сферы — 2 %.

Согласно проведенному опросу, практически всегда онлайн находятся 43% опрошенных, ежедневно пользуется интернетом 55 %, а несколько раз в неделю — 1 %. Частая активность в сети среди участников опроса представляет собой один из ключевых факторов, воздействующих на оценку актуальности цифровых сервисов. В большинстве областей развития сервисов более половины участников опроса считают эти сервисы полезными и актуальными. Однако стоит отметить, что в случае бизнес-сервисов данная тенденция нарушается из-за небольшой доли предпринимателей среди участников в общей выборке.

В исследовании также было рассмотрено, какие порталы используют жители для взаимодействия с органами власти. Госуслуги оказались наиболее популярным порталом, менее популярны площадки для размещения инициатив и голосования по ним. Помимо этого, активно используются офлайн каналы, например, личные встречи и многофункциональные центры.

Исследование показало, что среди опрошенных 74 % предпочитают использовать электронные формы для получения государственных услуг, 49% пользуются онлайн-платформы для решения городских вопросов, 42% активно участвуют в голосованиях по проектам и инициативам, 39 % подают жалобы на действия властей или уполномоченных организаций, 42% обращаются к органам власти для получения информации. Была обнаружена связь между уровнем уверенности респондентов во владении информационно-коммуникационными технологиями и тем, как они оценивают финансовое положение своих семей (двусторонняя корреляция Спирмена). Также было выявлено, что существует связь между использования Интернета и ИКТ и удовлетворенностью от жизни респондентов: чем больше пользователь уверен в своих ИТ-навыках, тем выше удовлетворенность жизнью.

Другой выявленной в ходе исследования закономерностью является доверие к взаимодействию с органами власти через средства Интернет-технологий. Жители с более высоким уровнем достатка склонны доверять такую типу взаимодействия. Люди, которые проявляют большее доверие к онлайн-взаимодействию с государственными органами, также испытывают большее удовлетворение от жизни и имеют убеждение в улучшении своего положения в ближайшем будущем.

Помимо этого, результаты показали взаимосвязь между тем, как респонденты оценивают эффективность функционирования сервисов, и параметрами их социального самочувствия. Среди участников, которые признают, что электронные сервисы способствуют более эффективному решению их проблем, отмечается более высокий уровень удовлетворенности жизнью. Кроме того, жители, которые верят в то, что Интернет-сервисы повышают общую удовлетворенность граждан от политических решений, также испытывают более высокий уровень удовлетворенности своей жизнью.

Исследование подтвердило гипотезу о взаимосвязи между использованием цифровых сервисов и уровнем социального самочувствия населения. Результаты онлайн-опроса выявили несколько факторов, которые связаны с этой взаимосвязью: уверенность в собственных ИТ-навыках, удобство цифровых сервисов, доверие к онлайн-взаимодействию с органами власти и оценка эффективности работы сервисов. Несмотря на существующие ограничения, связанных с таким типом опросов и ведущих к смещению выборки в пользу более активных интернет-пользователей, акцент на этой группе позволил получить ценные данные о взаимосвязи между цифровыми сервисами и социальным самочувствием. Офлайн-опрос даст возможность изучить различия между разными группами пользователей цифровых сервисов. Важным аспектом развития исследования также является разработка и операционализацией понятия «социальное самочувствие».

В будущем планируется разработать методику многофакторной оценки социального самочувствия. Эта методика будет использовать данные из социальных медиа и других доступных источников, что позволит провести тестирование разнообразных гипотез.

Исследование выполнено при поддержке Российского научного фонда и Санкт-Петербургского научного фонда, грант № 23-28-10069 «Прогнозирование социального самочувствия с целью оптимизации функционирования экосистемы городских цифровых сервисов Санкт-Петербурга» (https://rscf.ru/project/23-28-10069/).

СПИСОК ЛИТЕРАТУРЫ

1. Bimber B. The Internet and Political Transformation: Populism, Community and Accelerated Pluralism // Polity. 1998. Vol. 31 (1). P. 133-160.
2. Каргаполова Е. В. Социальное самочувствие населения: региональный аспект // Вестник Тюменского государственного университета. 2011. № 8. С. 80-86
3. Zhang Z., Zhang J., Zhao N., Yang Y. Social Network Size and Subjective Well-Being: The Mediating Role of Future Time Perspective Among

Community-Dwelling Retirees // Frontiers in Psychology. 2019. Vol. 10. Art. 2590. DOI: 10.3389/fpsyg.2019.02590 URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2019.02590/full
4. Vidiasov E., Vidiasova L., Tensina I. Institutional Factors for Building Trust in Information Technology: Case-Study of Saint Petersburg // Communications in Computer and Information Science. 2022. Vol. 1503. P. 152-162
5. Социальное самочувствие россиян: мониторинг. ВЦИОМ. 2021 г. https://wciom.ru/analytical-reviews/analiticheskii-obzor/socialnoe-samochuvstvie-rossijan-monitoring
6. Фантаццини Д., Шаклеина М. В., Юрас И. А. Big Data в определении социального самочувствия населения России // Прикладная эконометрика. 2018. № 2(50). С. 43–66.

УДК 34.096

ПРАВО НА ОТКАЗ ОТ ЦИФРОВЫХ ТЕХНОЛОГИЙ В УСЛОВИЯХ ДИНАМИЧНОЙ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

Денисов Денис Сергеевич
Университет ИТМО
Кронверкский пр., 49, лит. А, Санкт-Петербург, 197101, Россия
e-mail: dsdenisov@itmo.ru

Аннотация. Представляются результаты исследования, посвященного праву на отказ от цифровых технологий. На основе анализа академических, нормативных, аналитических и иных источников показано, что несмотря на наличие ряда существенных аргументов в пользу её развития, концепция права человека не использовать цифровые технологии и не подвергаться их воздействию при взаимодействии с государством и обществом находит слабое выражение как в доктрине, так и в нормативной среде. Формулируется вывод о том, что на фоне проблем цифрового неравенства и высокого уровня рисков, сопровождающих внедрение новых цифровых технологий, отсутствие таких правовых гарантий ставит под угрозу соблюдение важнейших прав и интересов человека.

Ключевые слова: право на отказ от цифровых технологий; цифровое неравенство; цифровая эксклюзия; цифровые платформы; цифровые экосистемы; цифровизация; регулирование; право; общество; власть.

THE RIGHT TO REFUSE DIGITAL TECHNOLOGIES IN THE CONTEXT OF DYNAMIC DIGITIZATION OF SOCIETY

Denisov Denis
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mail: dsdenisov@itmo.ru

Abstract. The results of the study on the right to refuse digital technologies are presented. Based on the analysis of academic, normative, analytical, and other sources, it is shown that even though there are substantial arguments for its development the concept of the human right not to use or to be affected by digital technologies in interaction with the state and society is poorly expressed both in the doctrine, and in the regulation. It is concluded that, given the challenges of digital inequality and the high level of risks that accompany the introduction of new digital technologies, the absence of such legal safeguards threatens fundamental human rights and interests.

Keywords: the right to refuse digital technologies; digital divide; digital exclusion; digital platforms; digital ecosystems; digitalization; regulation; law; society; authority; business.

Право пользоваться благами научного прогресса предусмотрено Всеобщей декларацией прав человека, и его значимость как для отдельных людей, так и для мирового сообщества сложно переоценить [1]. При этом в условиях динамичного развития сферы высоких технологий и постоянно растущей тенденции к цифровизации различных отраслей общественной жизни возникает закономерный вопрос: следует ли из этого права другая правовая возможность, а именно право человека отказаться от использования современных технологических решений при взаимодействии с государством и обществом?

Анализ академических источников показывает, что проблематика, связанная с обоснованием права на отказ от использования цифровых технологий, остается недостаточно разработанной. Немногочисленные исследования, прямо или косвенно затрагивающие этот вопрос, обосновывают необходимость существования такого права как техническими и социальными, так и этическими факторами. Например, авторы доклада РАНХиГС «Этика и «цифра»: от проблем к решениям» отмечают, что необходимость предоставления гражданам возможности свободно по собственному желанию выбирать аналоговую альтернативу цифровым сервисам и не подвергаться при этом дискриминации обусловлена не только проблемами пониженного доступа определенных групп населения к цифровым технологиям и ограниченной способности отдельных людей пользоваться электронными услугами, но и наличием нестандартных ситуаций вроде отключения электричества или сбоя в цифровой системе, а также потенциальной уязвимостью определенных цифровых технологий [2]. Исследователи обращают внимание на то, что задачами цифровизации являются ускорение, упрощение и удешевление процессов, при этом повсеместный переход на «цифру» без сохранения аналоговой альтернативы прямо противоречит указанным задачам, так как порождаемая им «цифровая сегрегация» приводит именно к затруднению получения некоторыми категориями граждан соответствующих услуг [2].

В качестве проблемы рассматривается не только уязвимость, но и опасность современных информационных технологий. Так, В.Б. Наумов сравнивает их с «черными ящиками», детального и достоверного представления о работе которых нет ни у общества, ни у государства, ни даже у разработчиков (в силу технической сложности разрабатываемых ими решений. Представляется, что в условиях неопределенности рисков участие человека и гражданина в «цифровых» правоотношениях должно быть добровольным, осознанным и предполагающим возможность отказаться от использования определенных технологий, при этом должна быть обеспечена система защиты прав лиц, не имеющих возможности, не желающих или опасающихся использовать новые сложные технологические решения [3].

Встречается и чисто правовая аргументация в пользу развития института права на отказ от цифровых технологий. Например, А.А. Волос и А. А. Иванов утверждают, что право на цифровизацию, понимаемое как субъективное право любого лица на восприятие и применение норм права при помощи цифровых средств, включая право на отказ от использования последних, уже предусмотрено Конституцией Российской Федерации, логически проистекает из совокупности её норм, предусматривающих возможность использования не запрещенных законом способов осуществления права, и требует при этом дальнейшего развития и конкретизации в актах Конституционного Суда Российской Федерации [4]. Допустимость отказа от использования цифровых технологий обосновывается авторами необходимостью существования гарантий, предусматривающих выбор средств и методов осуществления субъектами своих прав. При этом, с точки зрения исследователей, право на отказ от цифровизации не должно осуществляться произвольно, поэтому подлежат выработке принципы и основания его ограничения [4].

Право человека по его выбору не подвергаться воздействию тех или иных цифровых технологий нашло отражение и в ряде официальных документов. Например, Руководящие принципы 04/2020 по использованию данных о местоположении и средств по отслеживанию контактов в контексте вспышки COVID-19, утвержденные Европейским советом по защите данных, устанавливают, что использование приложений, отслеживающих контакты людей с целью минимизации распространения COVID-19, должны использоваться строго на добровольной основе, при этом лица, которые примут решение не использовать такие приложения, не должны подвергаться каким-либо неблагоприятным последствиям в результате своего выбора [5]. Это правило обосновывается тем, что что систематический и широкомасштабный мониторинг местонахождения и (или) контактов, происходящих между физическими лицами, является серьезным вмешательством в их частную жизнь.

Наиболее четко, последовательно и комплексно право на отказ от цифровых технологий было рассмотрено Советом при Президенте Российской Федерации по развитию гражданского общества и правам человека — сначала в докладе на тему «Цифровая трансформация и защита прав граждан в цифровом пространстве», а затем в проекте концепции обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве. В рамках этого проекта используется термин «цифровой суверенитет», который среди прочего предполагает право человека полностью или частично отказаться от вовлечения в цифровое взаимодействие, а также иметь возможность осуществлять свои права в отношении государства и общества вне цифрового пространства. По мнению авторов, дело не только в социальной недопустимости «цифровой эксклюизии», но и в естественно-правовом, конституционном характере права любого гражданина не пользоваться технологиями, которое, тем не менее, следует явно и недвусмысленно зафиксировать в законодательстве.

Тем временем в реальной жизни цифровизация наступает ускоренными темпами, причем как в государственном, так и в частном секторе. Отсутствие правовых гарантий нецифрового способа взаимодействия с государством и обществом осложняется принятием нормативных правил, прямо исключающих аналоговую альтернативу.

Стоит отметить, что позиция о недопустимости или нежелательности развития института «права на отказ от технологий» в профильных публикациях не обнаружена. Встречаются лишь доводы в пользу его ограничения или концепции, подразумевающее применение такого права только к определенным цифровым технологиям, например, к технологиям искусственного интеллекта. Но как таковой институт «права на отказ от технологий» доктринально не разработан. Тем не менее, необходимо констатировать, что отсутствие в правовом поле четко и недвусмысленно сформулированного права на отказ от использования цифровых технологий оставляет соблюдение важнейших прав и интересов человека на откуп исключительно воле «цифровизаторов» (в нынешних реалиях прежде всего власти государства и цифровых экосистем/платформ), которые по собственному усмотрению будут предоставлять или не предоставлять гражданам возможность участвовать в различных процессах нецифровым способом. Кроме этого, нет никаких гарантий, что выбор «нецифровой» («аналоговой») альтернативы, даже если таковая и будет предусмотрена, не поставит её пользователей в несоизмеримо худшее положение по сравнению с участниками так называемых «цифровых» отношений. На фоне проблем цифрового неравенства и высокого уровня рисков и угроз, сопровождающих внедрение новых цифровых технологий, такое положение дел способно обернуться масштабными негативными последствиями как для общества (государства) в целом, так и для человека (гражданина) в частности.

СПИСОК ЛИТЕРАТУРЫ

1. Всеобщая декларация прав человека. Принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года. [Электронный ресурс]. URL: https://www.un.org/ru/documents/decl conv/declarations/declhr.shtml (дата обращения: 10.09.2023).
2. Этика и «цифра»: от проблем к решениям. М. : РАНХиГС, 2021. 184 с.
3. Наумов В.Б. Отказ от цифровых технологий: абсурд или новое право человека и гражданина // Четвертые Бачиловские чтения: материалы

Международной научно-практической конференции. М.: Институт государства и права РАН, 2022. С. 78-84.
4. Волос А.А., Иванов А.А. Цифровизация и Конституция // Закон. 2022. № 12. [Электронный ресурс]. Доступ из СПС «Консультант Плюс» (дата обращения: 10.09.2023).
5. Руководящие принципы 04/2020 по использованию данных о местоположении и средств по отслеживанию контактов в контексте вспышки COVID-19. Утверждены Европейским советом по защите данных 21 апреля 2020 г. 19 с. [Электронный ресурс]. URL: https://edpb.europa.eu/sites/default/files/files/file1/dpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (дата обращения: 10.09.2023).
6. Проект концепции обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации. [Электронный ресурс]. URL: https://rocit.ru/uploads/4f68dc0a2487678a7675ad7589280277050b4004.docx?t=1639585614 (дата обращения: 10.09.2023).

УДК 323.213

РАЗРАБОТКА ЦИФРОВЫХ СЕРВИСОВ ПО ОПТИМИЗАЦИИ РАСХОДОВ ГОРОДСКОГО БЮДЖЕТА НА ФИНАНСИРОВАНИЕ ФАРМАКОТЕРАПИИ ДЛЯ ПАЦИЕНТОВ С ОНКОЛОГИЧЕСКИМИ ЗАБОЛЕВАНИЯМИ

Каневский Максим Александрович
Общество с ограниченной ответственностью «ГАЙКА ГРУПП»
Лифляндская ул., 3, лит. А, оф. 16, Санкт-Петербург, 190020, Россия
email: maxkanevsky@narod.ru

Аннотация. Развитие систем цифрового здравоохранения на основе экономики данных создает новые возможности для электронного партнерства в создании новых сервисов между государственными и частными ИС. Приведен пример использования платформы PharmBudget для оптимизации расходов городского бюджета на фармакотерапию пациентов с онкологическими заболеваниями.

Ключевые слова: электронные сервисы; цифровое здравоохранение; экономика данных.

DEVELOPMENT OF DIGITAL HEALTH SERVICES TO OPTIMIZE CITY BUDGET COSTS FOR FINANCING PHARMACOTHERAPY FOR PATIENTS WITH ONCOLOGICAL DISEASES

Kanevsky Maxim
Limited liability company Gaika Group (Gaika group Ltd.),
Liflyandskaya street, 3, lit. A, of. 16 St. Petersburg, 191020, Russia
email: maxkanevsky@narod.ru

Abstract. The development of digital health systems based on the data economy creates new opportunities for electronic partnerships in the creation of new services between public and private information systems. An example of using the PharmBudget platform to optimize city budget expenditures on pharmacotherapy for patients with cancer is given.

Keywords: e-services; digital health; data economics.

С развитием цифровых технологий и доступности медицинских данных, возникает уникальная возможность для государственных и частных информационных систем в сфере здравоохранения объединить свои усилия и создать инновационные сервисы. Одним из таких решений стала платформа PharmBudget, которая эффективно использует экономику данных для оптимизации расходов городского бюджета на фармакотерапию пациентов с онкологическими заболеваниями.

Ключевой функционал PharmBudget — анализ огромного количества вариантов распределения средств на терапию онкобольных на основе клинических рекомендаций Министерства здравоохранения РФ, профиля пациентов и доступного бюджета. Платформа позволяет проводить расчеты оптимального бюджета для проведения химиотерапии, учитывая специфику каждого случая и предоставляя возможность индивидуализированного подхода к лечению [1].

Апробация системы была проведена в профильном медицинском учреждении для пациентов с диагнозами рак молочной железы, раком яичников и меланома. В результате определены следующие основные преимущества:

1. Эффективное управление затратами. Оптимизация расходов на фармакотерапию, учитывая специфику заболевания и потребности каждого пациента. Это значительно снижает издержки и обеспечивает более рациональное использование бюджетных средств.

2. Индивидуализированный подход. Учет в протоколах лечения для разных видов рака, что позволяет предоставлять каждому пациенту оптимальный курс терапии, максимизируя шансы на выздоровление.

3. Экономический эффект. Экономия от 25% в зависимости от вида онкологического заболевания. Это означает существенные сбережения для городских бюджетов при сохранении высокого уровня медицинского обслуживания.

4. Повышение доступности лечения. Благодаря оптимизации расходов существенно повышается доступность лечения для большего числа пациентов.

Использование платформы требует 3 слоя данных: сведения о профиле и количестве пациентов из ЛПУ, сведения о бюджете из организации, определяющей финансирование, это может быть ЛПУ, так и профильные организации, например, Комитет по здравоохранению и сведения вариантах и стоимости терапии. Наладить информационный обмен можно в режиме онлайн в реальном времени или последовательно. Учитывая, что в ЛПУ установлены МИС, создается файл для передачи сведений в PharmBudget по API. Далее представитель

организации, ответственный за формирование бюджета, в интерфейсе PharmBudget или в своей основной рабочей ИС осуществляет необходимые расчеты.

Подобные платформы упрощают взаимодействие между представителями медицинского сообщества и финансистами, способствуют развитию научных исследований, обмену знаний и опытом между врачами и улучшению качества жизни пациентов и являются вдохновляющей иллюстрацией того, как современные технологии могут изменить облик медицины, делая ее более доступной, эффективной и персонализированной.

СПИСОК ЛИТЕРАТУРЫ

1. Константинова Ю. С., Каневский М. А. Гибридная автоматизированная оценка клинико-экономической эффективности противоопухолевой лекарственной терапии меланомы с учетом молекулярно-генетических особенностей опухоли и функционального статуса пациента // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2022. № 12. С. 171-176.
2. Свидетельство 2022611871 выдано 02.02.2022 Федеральной службой по интеллектуальной собственности. PharmBudget™. Программа для ЭВМ. URL: https://www1.fips.ru/registers-doc-view/fips_servlet? DB=EVM&DocNumber=2022611871&TypeFile=html (дата обращения: 01.09.2023).

У УДК 323.213

ВОСПРИЯТИЕ ЦИФРОВЫХ ГОСУДАРСТВЕННЫХ СЕРВИСОВ ГРАЖДАНСКИМИ АКТИВИСТАМИ САНКТ-ПЕТЕРБУРГА

Киселева Дарья Александровна[1,2], Сунгуров Александр Юрьевич[1,2]
[1] Высшая школа экономики,
Грибоедова канала наб., 123, Санкт-Петербург, 190068, Россия
[2] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: kiseleva-d@yandex.ru, asungurov@mail.ru

Аннотация. Тезисы представляют результаты исследования опыта взаимодействия гражданских активистов с цифровыми сервисами, а также их предпочтений относительно развития интернет-сервисов в Санкт-Петербурге. Выводы основаны на результатах двух анкет, заполненных представителями общественных организаций, а также на серии полуструктурированных интервью с гражданскими активистами и взаимодействующими с ними муниципальными депутатами.

Ключевые слова: цифровые сервисы; электронное правительство; гражданское общество; взаимодействие власти и общества.

PERCEPTION OF DIGITAL PUBLIC SERVICES BY CIVIL ACTIVISTS OF ST. PETERSBURG

Kiseleva Darya[1,2], Sungurov Alexander[1,2]
[1] HSE University, St. Petersburg,
Griboedova canal Emb, 123, St. Petersburg, 190068, Russia
[2] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: kiseleva-d@yandex.ru, asungurov@mail.ru

Abstract. The theses present the results of a study of experience of civil activists' interaction with digital services, as well as their preferences regarding the development of Internet services in St. Petersburg. The conclusions are based on the results of two questionnaires filled out by representatives of public organizations, as well as on a series of semi-structured interviews with civil activists and municipal deputies interacting with them.

Keywords: digital services; e-government; civil society; interaction between the government and society.

В рамках сообщения будут представлены первые результаты исследовательского проекта, посвященного изучению социальной результативности электронного взаимодействия граждан и власти в Санкт-Петербурге на примере городских цифровых сервисов [1]. Одним из направлений проекта было выявление отношения к этим цифровым сервисам активистов городских общественных организаций и движений. Первым мероприятием в рамках реализации этого направления было проведение 21 апреля 2023 года на площадке НИУ ВШЭ — СПб круглого стола на тему «Гражданское общество и городская власть: формы взаимодействия», на который были приглашены представители многих городских общественных организаций. Интерес к этой группе граждан и тематике мероприятия возник в связи с тем, что в существующих исследованиях, посвященных электронным сервисам и электронному участию, анализируются технические стороны работы электронных сервисов, нюансы внедрения электронного участия [1, 2], однако, помимо эффектов от уже существующих каналов электронного участия, нам хотелось узнать об ожиданиях граждан от текущего развития интернет-сервисов. При этом в подобных исследованиях общественного мнения активисты и общественные организации, как правило, не выделяются в отдельную группу со своими потребностями и опытом использования интернет-сервисов, в то время как, очевидно, их заинтересованность в использовании всех каналов коммуникации с властью выше, чем у рядовых граждан, а запрос на сервисы, помогающие в продвижении идей организованных групп отличается от запроса сервисов для удовлетворения личных потребностей граждан (например, запись к врачу). Необходимость

учета мнения активистов подтверждается и результатами исследования проблем внедрения и функционирования каналов электронного участия, в ходе которого активисты характеризовали существующие каналы как продуктивные «для решения самых примитивных проблем» и созданные «для людей, которые не разбираются» [3]. Именно поэтому в данном исследовании мы изучили взгляд активистов и представителей общественных организаций на цифровые сервисы Санкт-Петербурга. В рамках дискуссии на круглом столе обсуждались успехи, неудачи и тактики гражданского активизма, направленного на решение проблем создания благоприятной и экологичной городской среды. В ходе обсуждения участникам круглого стола был также представлен проект «Исследование социальной результативности электронного взаимодействия граждан и власти в Санкт-Петербурге на примере городских цифровых сервисов (2023–2025). Помимо мнений, озвученных в ходе мероприятия, мы получили следующие данные.

Для начала участникам мероприятия было предложено две анкеты — первая, «входная», которую они заполняли перед началом круглого стола, и вторая, заполнявшаяся участниками после завершения его работы. Затем в течении полутора месяцев после этой встречи были проведены экспертные полуструктурированные интервью, респондентами которых были как участники круглого стола, так и рекомендованные ими активисты НКО, а также два муниципальных депутата, тесно взаимодействующие с гражданскими активистами. В ходе интервью попросили респондентов рассказать о своей деятельности, об отношении к интернет-сервисам и использовании их в своей общественной работе, а также подумать о том, какие сервисы для активистов они предложили бы создать. Всего было взято шестнадцать таких интервью.

Обработка анкет выявила, что городские интернет-сервисы знают все пятнадцать человек, ответивших на первую анкету, при этом примерно треть назвала по пять таких сервисов. Наиболее часто назывался портал «Наш Петербург» и «Госуслуги СПб (по 5 чел.), «Здоровье петербуржца» (4 чел.), «Доступная среда» и «Карта ответственности» (по 3 чел.), «Госуслуги РФ» и ГИС ЖКХ (по 2 чел.).

На вопрос «Какие интернет-сервисы следовало бы, на Ваш взгляд, развивать в Санкт-Петербурге?» пятеро респондентов ответили так: коммуникации, диалога; достойный петербургский аналог «Активного гражданина», гражданское участие; портал по внесению предложений по общественным инициативам; СМИ и городских проблем. Два человека предложили развивать сервисы, связанные с работой городского транспорта: «Необходим городской сервис по отслеживанию городского транспорта (работающий хорошо, а не как существующие сейчас)», еще двое — с медициной (качество приема в медучреждениях, запись в медицинские организации), и еще двое — сервисы, посвященные правовой информации, поясняющие права и обязанности жителей города. По одному человеку назвали в качестве приоритетных интернет-сервисов назвали «Твой бюджет», «Карта ответственности», Туристические маршруты и маркетплейсы.

Анализ текстов экспертных интервью показал, что среди респондентов есть как люди, знающие о существовании городских цифровых сервисах и использующие их в своей жизни, так и те, кто не придает этим сервисам большого значения или относится к ним критически. Так, респондент А утверждает: «У меня был опыт использования, это был опыт оформления больничного. Я сделала это через бот, потом дальше я просто знаю, что есть платформа «Я здесь живу» в «ВКонтакте», там есть разные роли, где можно выбрать роль. Можно посмотреть для себя какие-то мероприятия, предложения и прочее., но сама этим сервисом не пользовалась, не щупала, наверное, в силу того, что я в принципе знаю, что происходит в городе, где что найти и как кому обратиться». Таким образом, мы видим, что для более активных людей, привыкших получать информацию в достаточном объеме из других источников, информационные сервисы не имеют большой значимости, однако далее респондент дает пояснение, что другим людям их, конечно, стоит порекомендовать и, более того, было бы лучше, если бы их рекламировали активнее: «Будучи очень подвижным человеком, метро автобусы — вот это вот всё, я редко вижу рекламу городских сервисов, точнее, я её практически не вижу. […] Поскольку я не очень сейчас представляю, какие есть принципы сервисы, то есть мне нужно с ними ознакомиться более подробно погрузиться в это, то я бы начала действительно с очень хорошей информационной кампании».

Респонденты Б и В называют ещё одну причину, по которой активисты не используют электронные сервисы — для их деятельности нужны прямые контакты с людьми, а электронные сервисы не представляются им надежными и нужными каналами для коммуникации («поскольку мы часто общаемся с чиновниками разными, то какой смысл писать чрез какие-то сервисы, когда проще спросить напрямую у ответственного лица и сразу будет понятно, сделают они что-то или не сделают»). Однако респондент Б всё же смог назвать сервисы, которые пригодились бы активистами. Во-первых, он предложил перенять опыт столицы и создать похожие сервисы для Петербурга: «в Москве есть такой сервис «Активный гражданин», но у нас ничего подобного нет». Во-вторых, он предложил сервис, способный упростить работу активистов: «Хорошо бы перевести в интернет процесс согласования наших мероприятий. Ну вот какие-то там забеги, субботники — все эти мероприятия по действующему законодательству требуют согласований. И это сделать сейчас практически невозможно. Так вот сделать бы интернет-сервис для согласования подобных мероприятий, например, акций, когда идет речь о массовых или не очень массовых мероприятий — это было бы замечательно».

В завершение приведем фрагмент из интервью с респондентом В, которая уже имеет опыт обсуждении электронных сервисов: «Несколько лет тому назад, до COVID-19, я участвовала в каких-то совещаниях по созданию интернет-сервисов, и тогда я говорила о необходимости создания площадок для диалога между представителями власти и гражданскими организациями, бизнес-ассоциациями, иначе говоря, социально неравнодушными людьми, которые бы знакомили представителей власти с реальными проблемами, которые накапливаются в обществе, и совместно бы искали пути их решения. К сожалению, наши пожелания не были

восприняты, и система городских цифровых сервисов была создана не для активных граждан, а для потребителей тех или иных услуг». Мы можем заключить, что общественные активисты не считают, что существующие электронные сервисы отвечают их потребностям рассчитывают на появление новых, полезных для них площадок.

Исследование выполнено за счет гранта Российского научного фонда и Санкт-Петербургского научного фонда № 23-18-20079 «Исследование социальной результативности электронного взаимодействия граждан и власти в Санкт-Петербурге на примере городских цифровых сервисов» (https://rscf.ru/project/23-18-20079/).

СПИСОК ЛИТЕРАТУРЫ

1. Цифровые городские сервисы в системе регионального управления (на примере экосистемы городских сервисов Санкт-Петербурга) / Минаев Н. Н. [и др.] // Региональная экономика: теория и практика, 2023. Вып. 10.
2. Чугунов А. В., Кабанов Ю. А., Панфилов Г. О. Мониторинг ресурсов электронного участия в России // Государство и граждане в электронной среде. Выпуск 4 (Труды XXIII Международной объединенной научной конференции «Интернет и современное общество», IMS-2020, Санкт-Петербург, 17–20 июня 2020 г. Сборник научных статей). СПб.: Университет ИТМО, 2020. С. 61–72.
3. Аркатов Д. А. Проблемы электронного гражданского участия в публичной политике города: случай Санкт-Петербурга // Политическая наука, 2022, № 3. С. 296–317.

УДК 004.9:351.9

АНАЛИЗ ВНЕДРЕНИЯ ЭКОСИСТЕМЫ ГОРОДСКИХ СЕРВИСОВ «ЦИФРОВОЙ ПЕТЕРБУРГ»

Кузнецов Алексей Геннадьевич
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: alexkuznec98@gmail.com

Аннотация. В работе проводится анализ внедрения экосистемы городских сервисов «Цифровой Петербург». По результатам анализа сделаны выводы о том, что «Цифровой Петербург» посредством реализации цифровых сервисов охватывает интересы самых различных групп населения, каждая из которых выполняет свою «социальную роль».

Ключевые слова: экосистема; социальная роль; цифровые сервисы; электронное управление.

ANALYSIS OF THE IMPLEMENTATION OF THE ECOSYSTEM OF CITY SERVICES «DIGITAL PETERSBURG»

Kuznetsov Aleksei
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mail: alexkuznec98@gmail.com

Abstract. The paper analyzes the ecosystem of network services «Digital Petersburg». Based on the results of the analysis, it was concluded that «Digital Petersburg» through the implementation of digital services provide the interests of various groups of the population capable of fulfilling their «social role».

Keywords: ecosystem; social role; digital services; e-government.

В настоящее время в Санкт-Петербурге внедряется экосистема городских сервисов (ЭГС) «Цифровой Петербург», которая нацелена на решение потребностей горожан самыми инновационными способами — используя нейросети, синтез речи, чат-боты и другие технологии [1]. ЭГС включает использование государственных и коммерческих сервисов жителями, направленное на развитие цифровой среды города и создания новых сервисов на базе открытых данных. Важно отметить, что ЭГС сформирована по принципу ролевой модели, которая сортирует сервисы под различные целевые аудитории и их потребности (например, «Я — родитель», «Я — работник, «Я за Спорт», «Я люблю Петербург» и др.).

В контексте анализа «социальной роли» и использования гражданами «цифровых сервисов» в докладе даются определение этих понятий. Социальная роль определяется как взаимодействие личности с обществом в результате которого воспроизводятся стереотипы (шаблоны) поведения, отвечающие его статусу в различных жизненных обстоятельствах (например, турист, спортсмен, учитель, экскурсовод и др.) [2]. В то же самое время цифровые сервисы определяются как комплексные решения, направленные на качественное улучшение или ускорение организационных или управленческих процессов с целью удовлетворения потребностей граждан и бизнеса [3].

На данный момент в ЭГС зафиксированы 26 ролей, которые разделены на шесть социальных сфер к каждой из которых «подключены» цифровые сервисы: «Мой дом — Петербург» (166 сервисов), «Мой отдых» (85 сервисов), «Моя работа» (47 сервисов), «Моя семья» (58 сервисов), «Моя учеба» (43 сервиса) и «Мое здоровье» (32 сервиса). В целом к экосистеме подключено 229 цифровых сервисов, из которых: 193 — сайты, 30 — чат-боты, Яндекс (навык Алисы) — 4, Приложение — 23, ВК мини-апп — 7, СМС -информирование-1. Общее количество уникальных посетителей сервисов ЭГС насчитывает 2,5 млн человек в неделю, что говорит о востребованности цифровых сервисов у граждан Санкт-Петербурга. Это подтверждает и количество социальных ролей, которое выросло за три года в три раза.

В рамках предпроектного обследования выявлено, что лидирующее место занимает сервис «Я здесь живу» (36 сервисов), «Я родитель» (34 сервиса), «Я турист» (27 сервисов), «Я гражданин» (26 сервисов). Самыми малочисленными сервисами являются «Я с дроном» (2 сервиса), «Я дачник» (4 сервиса), «Я экскурсовод» (4 сервиса). Это подтверждается и количеством охвата населения, которые могли бы воспользоваться данными сервисами. В частности, «Я здесь живу» имеет охват в 5,3 млн человек, «Я гражданин» — 2,5 млн. человек, в то время как «Я экскурсовод» — 6 тыс. человек, «Я с дроном» — 50 тыс. человек. Данные результаты исследования говорят о том, что ЭГС стремится охватить самые разные социальные роли жителей Санкт-Петербурга.

Таким образом, экосистема «Цифровой Петербург» позволяет удовлетворить потребности различных групп населения через цифровое взаимодействие. Дальнейшее исследование будет касаться изучения потребностей, связанных с «социальными ролями».

Исследование выполнено за счет гранта Российского научного фонда и Санкт-Петербургского научного фонда № 23-18-20079 «Исследование социальной результативности электронного взаимодействия граждан и власти в Санкт-Петербурге на примере городских цифровых сервисов» (https://rscf.ru/project/23-18-20079/).

СПИСОК ЛИТЕРАТУРЫ

1. Экосистема городских сервисов Цифровой Петербург. URL: https://about.petersburg.ru/ (дата обращения: 25.08.2023).
2. Vial A.C., Dovidio J.F., Brescoll V.L. Channeling others' biases to meet role demands // Journal of Experimental Social Psychology. 2019. Vol. 82. P. 47–63. DOI: 10.1016/j.jesp.2019.
3. Петров М., Буров В., Шклярук М., Шаров А. Государство как платформа: (кибер)государство для цифровой экономики. Цифровая трансформация [Электронный ресурс]. М., 2018. URL: https://www.csr.ru/upload/iblock/313/3132b2de9ccef0db1eecd56071b98f5f.pdf (дата обращения: 25.08.2023).

УДК 323.2

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ СЕРВИСОВ В МУНИЦИПАЛИТЕТАХ САНКТ-ПЕТЕРБУРГА

Метелева Алина Сергеевна[1], Слав Юлия Эдуардовна[2], Филатова Ольга Георгиевна[1,3]
[1]Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
[2]Совет муниципальных образований Санкт-Петербурга
пр. Металлистов, 93, лит. А, Санкт-Петербург, 195221, Россия
[3]Санкт-Петербургский государственный университет
Университетская наб., 7–9, Санкт-Петербург, 199034, Россия
e-mails: metelyovalina@mail.ru, info-sovetmo@yandex.ru, o.filatova@spbu.ru

Аннотация. Тезисы представляют результаты социологического исследования, посвящённого практике использования цифровых сервисов представителями органов местного самоуправления Санкт-Петербурга. Опрос показал, что большинство муниципальных служащим осведомлены о цифровых сервисах и используют их в своей работе; большинство муниципальных служащих считают цифровые сервисы эффективным инструментом при принятии решений и выстраивании коммуникации с жителями города.

Ключевые слова: цифровые сервисы; государственные электронные сервисы; экосистема городских сервисов.

THE USE OF DIGITAL SERVICES IN THE MUNICIPALITIES OF ST. PETERSBURG

Meteleva Alina[1], Slav Julia[2], Filatova Olga[1,3]
[1] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
[2] Council of municipalities of Saint Petersburg
93 Metallistov Av, lit. A, St. Petersburg, 195221, Russia
[3] Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mails: metelyovalina@mail.ru, info-sovetmo@yandex.ru, o.filatova@spbu.ru

Abstract. The theses present the results of a sociological study devoted to the practice of using digital services by representatives of local self-government bodies of St. Petersburg. The survey showed that most municipal employees are aware of digital services and use them in their work; most municipal employees consider digital services to be an effective tool in making decisions and building communication with city residents.

Keywords: digital services; public electronic services; urban services ecosystem.

Активное развитие интернет-технологий способствует появлению большого количества цифровых сервисов, используемых как гражданами, там и органами власти разного уровня. Как утверждалось в ряде предыдущих публикаций, в настоящее время можно говорить уже даже о формировании сравнительно целостной экосистемы электронного взаимодействия на местном, или «низовом», уровне [1-3]. С 24 июля по 16 августа был проведён социологический опрос, целью которого стало выявление отношения представителей муниципалитетов Санкт-Петербурга к цифровым сервисам, а также изучение успешности их применения в работе органов местного самоуправления. Опрос проводился Центром технологий электронного правительства Института дизайна и урбанистики Университета ИТМО совместно с Советом муниципальных образований Санкт-Петербурга. Под

цифровыми сервисами в данном опросе понималось комплексное решение на базе цифровых продуктов, направленное на качественное улучшение или ускорение организационных или управленческих бизнес-процессов (определение взято из доклада ООН 2022 года).

Респондентами опроса стали представители органов местного самоуправления (ОМСУ) Санкт-Петербурга. Всего на территории районов Санкт-Петербурга расположено 111 муниципальных образований, которые наделены статусами муниципального округа, города или посёлка. Общее количество муниципальных служащих, работающих в ОМСУ Санкт-Петербурга, составляет более полутора тысяч человек. Участниками данного опроса стал 101 муниципальный служащий из разных муниципальных образований Санкт-Петербурга. Опрос проводился на профессиональной платформе «Анкетолог».

Согласно проведённому опросу, о существовании городских цифровых сервисов осведомлены 90,1% муниципальных служащих, 87,9 % из них используют цифровые сервисы в своей работе. Большинство использующих цифровые сервисы в своей работе обращаются к ним часто (ежедневно) — 47,5 %. Меньшее количество муниципальных служащих отметили, что используют цифровые сервисы в работе более-менее регулярно (несколько раз в неделю) — 30%; редко (несколько раз в месяц) — 22,5 %. Чаще всего цифровые сервисы в своей работе используют респонденты, назвавшие своим профессиональным интересом благоустройство территории, — 34,2 % от обращающихся к цифровым сервисам ежедневно.

40 % респондентов используют в работе федеральные и региональные цифровые сервисы с примерно одинаковой частотой. 35 % опрошенных чаще обращаются к региональным цифровым сервисам, нежели федеральным; 25 % респондентов чаще обращаются к федеральным цифровым сервисам, нежели региональным.

В качестве конкретных цифровых сервисов, которые используются при реализации рабочих задач, чаще всего респонденты называли следующие ресурсы: Портал государственных услуг Российской Федерации (Госуслуги) (56,7 % опрошенных), Платформа обратной связи (ПОС) (53,7%), Региональная информационная система «Геоинформационная система Санкт-Петербурга» (РГИС) (37,3%), Портал «Наш Санкт-Петербург» (34,3%), Автоматизированная информационная система государственного банка о детях, оставшихся без попечения родителей (АИСТ ГБД) (10,4 %), Единая информационная система в сфере закупок (ЕИС) (10,4 %), Единая государственная информационная система социального обеспечения (ЕГИССО) (10,4 %).

В ряде вопросов предлагалось оценить практику использования цифровых сервисов представителями ОМСУ. Так, большинство респондентов — 93,1 % — согласны с утверждением, что использование в работе ОМСУ городских цифровых сервисов повышает качество предоставляемых услуг (варианты ответа «да» (38,6 %) и «скорее да» (54,5 %)). По мнению 77,2 % опрошенных, городские цифровые сервисы являются полезной разработкой, благодаря которой граждане получают возможность напрямую взаимодействовать с органами власти. 58,4% респондентов отметили, что использование городских цифровых сервисов повышает нагрузку на муниципальных и государственных служащих. 44,6% опрошенных не считают, что использование городских цифровых сервисов увеличивает временные и административные издержки при принятии решений.

84,1 % муниципальных служащих отметили, что городские цифровые сервисы можно назвать эффективным инструментом при принятии решений и выстраивании коммуникации с жителями города (варианты ответа «да» (27,7 %) и «скорее да, чем нет» (56,4 %)). По мнению же 18,9 % опрошенных городские цифровые сервисы не являются эффективным инструментом при принятии решений и выстраивании коммуникации с жителями города (варианты ответа «нет» (4 %) и «скорее нет, чем да» (11,9 %)).

Сторонники первой точки зрения чаще всего поясняли свой ответ следующим образом:

– цифровые сервисы экономят время как граждан, так и муниципальных служащих;
– цифровые сервисы удобны для коммуникации власти и общества;
– цифровые сервисы обеспечивают вовлечение жителей муниципального образования в управленческие процессы.

Сторонники противоположной версии в качестве пояснения своего мнения привели следующие доводы:

– цифровые сервисы могут быть сложны в использовании;
– цифровые сервисы не могут обеспечить реального диалога власти и общества в силу опосредованности коммуникации;
– цифровые сервисы не обеспечивают вовлечение граждан в управленческие процессы, практика их применения фиктивна.

Опрошенные считают, что на развитие городских цифровых сервисов могут оказать влияние такие факторы, как повышение цифровой грамотности населения (57,4%), реклама городских сервисов в общественных местах — (40,6%), появление новых сервисов, предлагающих удовлетворение новых потребностей (37,6%), снижение масштабов цифровых угроз населению (мошенничество, торговля данными) (35,6%), увеличение/уменьшение доверия граждан к власти (30,7%) и т.д. На вопрос, необходимо ли разрабатывать и внедрять отдельные городские сервисы для муниципалитетов, 73,3% респондентов ответили положительно (варианты ответа «да» (30,7%) и «скорее да, чем нет» (42,6%)). 49,5% муниципальных служащих считают, что внедрение городских цифровых сервисов в деятельность ОМСУ в формате, который реализован на уровне Санкт-Петербурга, возможно, но это потребует значительных ресурсов; 39,6% опрошенных считают, что такое внедрение возможно с минимальными ресурсами; 10,9% респондентов считают такое внедрение невозможным.

В продолжение исследования планируются экспертные интервью с отдельными представителями ОМСУ для выявления результативности и эффективности использования цифровых сервисов органами местной власти.

Исследование выполнено за счет гранта Российского научного фонда и Санкт-Петербургского научного фонда № 23-18-20079 «Исследование социальной результативности электронного взаимодействия граждан и власти в Санкт-Петербурге на примере городских цифровых сервисов» (https://rscf.ru/project/23-18-20079/).

СПИСОК ЛИТЕРАТУРЫ

1. Misnikov Y., Filatova O., Trutnev D. Empirical Modeling of e-Participation Services as Media Ecosystems // Social Computing and Social Media: Experience Design and Social Network Analysis. HCII 2021, Proceedings. Meiselwitz, G. (Eds). Springer Nature, Lecture Notes in Computer Science. 2021. Vol. 12774 LNCS. P. 87–104.
2. Мисников Ю.Г., Филатова О.Г. Развитие сервисов электронного участия на уровне местного самоуправления: медиаэкологический подход // Информационная безопасность регионов России (ИБРР-2021). XII Санкт-Петербургская межрегиональная конференция. СПб : СПОИСУ, 2021. С. 30–32.
3. Филатова О.Г. Публичная коммуникация граждан и органов местного самоуправления в экосистеме цифровых сервисов Санкт-Петербурга // Политические вызовы и политический диалог в условиях глобальной турбулетности. Материалы всероссийской конференции РАПН. М., 2022. С. 467–468.

УДК 323.213

ЭКОСИСТЕМА ГОРОДСКИХ СЕРВИСОВ «ЦИФРОВОЙ ПЕТЕРБУРГ»

Осмоловский Кирилл Евгеньевич [1, 2]
[1] СПб ИАЦ,
Транспортный пер., 6, лит. А, Санкт-Петербург, 191040, Россия
[2] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
email: kirillosmolovsky@mail.ru

Аннотация: Экосистема городских сервисов «Цифровой Петербург» — пространство взаимодействия государственных и коммерческих сервисов с жителями, направленных на развитие цифровой среды города, облегчение доступа к API органов власти для создания новых сервисов и проведения аналитики на базе открытых данных. В рамках экосистемы разработана ролевая модель.

Ключевые слова: экосистема городских сервисов; ролевая модель; открытые данные.

ECOSYSTEM OF CITY SERVICES «DIGITAL PETERSBURG»

Osmolovsky Kirill[1, 2]
[1] St. Petersburg State Unitary Enterprise SPb IAC,
6 Transportny l., lit. A, St. Petersburg, 191040, Russia
[2] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
email: kirillosmolovsky@mail.ru

Abstract. The ecosystem of city services «Digital Petersburg» is a space of interaction between government and commercial services with residents aimed at developing the digital environment of the city, facilitating access to the API of authorities for creating new services and conducting analytics based on open data. A role model has been developed within the ecosystem.

Keywords: ecosystem of urban services; role model; open data.

В городе проживают миллионы людей, и у каждого человека есть свои потребности [1]. На решение потребностей горожан Санкт-Петербурга ориентируется Экосистема городских сервисов «Цифровой Петербург» (далее — ЭГС), представляющая собой модель предоставления цифровых услуг или сервисов, расположенных в одном месте. Сервис может быть создан как государственными, так и коммерческими структурами.

К основным принципам ЭГС относятся инновационность (используются такие технологии, как чат-боты, нейросети и т. п.), ведение диалога с горожанами (частью ЭГС является конструктор чат-ботов, делающий возможным создание новых сервисов для решения актуальных проблем), открытость (проект доступен для сотрудничества с горожанами и готов включать необходимые им сервисы [3] в ЭГС — https://about.petersburg.ru/).

Для создания городских сервисов ЭГС предоставляет партнерам и разработчикам доступ к открытым данным через «одно окно». Эти данные (данные множества государственных информационных систем, партнерских сервисов и т.д.) в деперсонализированном виде предоставляет город через открытые API. Дальнейшая работа с данными строится на возможности подключения к API-шине ЭГС.

В качестве партнеров ЭГС привлекаются различные площадки, обладающие своей аудиторией и заинтересованные в повышении качества предоставляемых услуг. Например, такими партнёрами являются «ВКонтакте» и «Яндекс», с которыми у Санкт-Петербурга подписаны партнёрские соглашения. Благодаря этому данные из ЭГС об отключении горячей воды или передвижении общественного транспорта размещаются на «Яндекс Картах», что позволяет проинформировать бóльшую часть жителей.

В настоящий момент на портале ЭГС доступно 228 сервисов [2]. Сервисы создаются по результатам опросов жителей и консультаций с экспертами, после чего ведётся информирование жителей о доступности им определённых услуг через публикацию сведений о сервисах на портале ЭГС.

Одна из ключевых особенностей ЭГС — ролевая модель (сейчас представлено 23 роли, среди которых «Я — родитель», «Я — работник», «Я люблю книги» и т.д.) [2]. Использование ролевой модели в ЭГС даёт возможность учесть и охватить наибольшее число потребностей горожан, а также позволят пользователю упростить навигацию среди множества сервисов, таргетировать уведомления и подписки на актуальные темы.

В результате, город, его жители, бизнес-сообщества и просто энтузиасты получают возможность реализовать свои проекты и улучшить жизнь города, развивая цифровые сервисы и обогащая ЭГС новыми данными.

Исследование выполнено за счет гранта Российского научного фонда и Санкт-Петербургского научного фонда № 23-18-20079 «Исследование социальной результативности электронного взаимодействия граждан и власти в Санкт-Петербурге на примере городских цифровых сервисов» (https://rscf.ru/project/23-18-20079/).

СПИСОК ЛИТЕРАТУРЫ

1. Карчагин Е. В. Социальные потребности горожан: теоретико-методологические аспекты // Социология города. 2023. № 1. С. 5–19.
2. 228 городских сервисов «Цифрового Петербурга» работают для жителей // Администрация Санкт-Петербурга [Электронный ресурс]. URL: https://www.gov.spb.ru/gov/admin/kazarin-sv/news/263218/ (дата обращения: 04.10.2023).
3. Цифровой Петербург [электронный ресурс]. URL: https://about.petersburg.ru/ (дата обращения: 04.10.2023).

УДК 316.422.42

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЦИФРОВЫХ СЕРВИСОВ С УЧЕТОМ СПЕЦИФИКИ ДОВЕРИЯ ПОЖИЛЫХ ПОЛЬЗОВАТЕЛЕЙ К ОНЛАЙН-ПЛАТФОРМАМ

Равчик Михаил Игоревич
СИ РАН — филиал ФНИСЦ РАН,
Красноармейская 77-я, 25/14, Санкт-Петербург, 190005, Россия
e-mail: mravchik1@gmail.com

Аннотация. Рассматривается специфика доверия пожилых людей к цифровым сервисам в контексте цифровой безопасности. Выделяются следующие факторы, влияющие на субъективное ощущения доверия пожилых людей к цифровым сервисам: авторитетность и верифицируемость сервисов с традиционными организациями и институтами, а также субъективное ощущение отреченности от цифрового пространства, основанное на незнакомой для пожилых пользователей терминологии, используемой в интернет-пространстве. По результатам анализа сделан вывод, что обеспечение безопасности цифровых сервисов, ориентированных на пожилых пользователей, должно строиться не только на повышении объективных стандартов цифровой безопасности, но и повышении степени доверия пожилых людей к данным сервисам.

Ключевые слова: цифровые сервисы; пожилые люд; доверие; цифровая безопасность.

ENSURING THE SECURITY OF DIGITAL SERVICES WITH CONSIDERATION FOR THE TRUST SPECIFICS OF ELDERLY USERS TOWARDS ONLINE PLATFORMS

Ravchik Mihail
SI RAS - branch of the FNISC RAS,
25/14 Krasnoarmeyskaya 77th, St, St. Petersburg, 190005, Russia
e-mail: mravchik1@gmail.com

Abstract. The specificity of trust among elderly individuals towards digital services is examined within the context of digital security. The following factors influencing the subjective sense of trust among elderly individuals towards digital services are highlighted: the credibility and verifiability of services in comparison with traditional organizations and institutions, as well as the subjective feeling of detachment from the digital realm, rooted in unfamiliar terminology used within the internet space, which is unfamiliar to elderly users. Based on the analysis, the conclusion is drawn that ensuring the security of digital services tailored to elderly users should be built not only on the enhancement of objective digital security standards but also on increasing the level of trust that elderly individuals have in these services.

Keywords: digital services; elderly people; trust; digital security.

Несмотря на стабилизацию демографических процессов, тенденция увеличения доли пожилых людей в возрастной структуре населения сохранится [1]. В данном контексте вопрос обеспечения безопасности цифровых сервисов становится все более актуальным, так как напрямую влияет на степень включенности пожилых людей в интернет-пространство. Широкие возможности осуществлять выбор, связанные с большим количеством цифровых сервисов, позволяют составить пожилому человеку индивидуальный план старения, основанный на собственных потребностях и не ограниченный различными институциональными барьерами. Однако, несмотря на подобные возможности, нынешние поколения пожилых людей остаются одной из самых низко вовлечённых в цифровую среду демографических групп. Регулярно публикуемые статистические данные позволяют нам увидеть рост количества пожилых пользователей Интернетом, при этом в сравнении с другими возрастными группами количество и качество цифровых взаимодействий все еще находятся на низком уровне [2].

В первую очередь попытаться найти причины такой низкой вовлеченности можно в плоскости низкой компьютерной грамотности данной возрастной группы. Тем не менее, исследователи отмечают, что пожилые, даже после прохождения обучающих курсов компьютерной грамотности, редко продолжают обращаться к цифровым сервисам в повседневной жизни, что позволяет нам предположить, что освоение соответствующих компетенций не является само по себе причиной для тесного дальнейшего взаимодействия с Интернет-пространством [3], это лишь необходимое условие для такого взаимодействия, достаточное же условие — доверие пожилых людей к цифровому пространству. Доверие пожилых к цифровым сервисам является одним из важнейших компонентов мотивации к включению во взаимодействие на онлайн-платформах. Как нам видится,

обеспечение безопасности цифровых сервисов является обязательным условием возникновения доверия и должно строиться не только на развитии объективных мер обеспечения безопасности платформ, но и на повышении субъективного ощущения включенности, привычной для пользователя атмосфере.

Цифровая среда доверия пожилых людей в большей степени чем у других возрастных групп базируется на паттернах доверия, основанных на взаимодействии с традиционными нецифровыми сервисами. Однако в случае пожилых людей можно наблюдать непонимание его границ [4]. Нередко случаются ситуации, при которых пожилой полностью доверяет работе определенного учреждения, но при этом отказывается доверять официальному сайту данной организации, предпочитая нецифровое взаимодействие. Мы предполагаем, что подобное явление напрямую связанно со слабым пониманием авторитета субъектов цифровых взаимодействий. Пожилые люди не распространяют авторитет традиционных организаций в интернет-пространство. Вместо этого в глазах пожилых людей возникают два субъекта — организация и её сетевой двойник. Но степень авторитета данных субъектов отличается. Авторитет традиционной организации основывается на предыдущем опыте взаимодействия с ней, на том, что пожилой «знает» эту организацию и конкретные учреждения, связанные с ней. В случае с цифровыми сервисами, связанными со знакомыми организациями, небольшой сетевой опыт пожилых негативно влияет на степени их доверия к ним. При этом, также можно наблюдать и обратную ситуацию, при которой отсутствие опыта и связанное с ним понимание авторитета субъектов онлайн-взаимодействия приводит к безосновательному доверию. Подобное доверие может быть основано на схожих позициях и убеждениях, ретранслируемых данным субъектом. Ярким примером этому могут служить ситуации, часто возникающие в информационном пространстве, в которых пожилые люди предпочитают доверять первому увиденному источнику информации в Интернете, игнорируя альтернативные точки зрения. Основываясь на этом, для обеспечения безопасности цифровых сервисов для пожилых людей провайдерам услуг необходимо основывать свой авторитет на уже существующих традиционных организациях, знакомым пожилым. В контексте цифровых экосистем необходимо создать явную корреляцию между самой экосистемой, а также включенными в нее сервисами, с государственными институтами, отвечающими как за цифровизацию, так и за специфические сферы онлайн-потребления (например, подтверждать верифицированность цифровых сервисов здравоохранения посредством одобрения от Министерства здравоохранения и т.п.).

Навыки компьютерной грамотности также влияют на доверие пожилых людей к цифровым сервисам. Однако наличие навыков по работе с компьютерной техникой не влияет в той же степени на доверие, как отсутствие навыков цифровой грамотности [5]. Неразвитые навыки обработки многообразия информации в Интернете, часто носящей противоречивый характер, приводит к снижению доверия пожилых к цифровому пространству в целом, и сервисам в частности [6]. Интернет для пожилых людей — незнакомое пространство, в котором пожилые люди сталкиваются с другими видами взаимодействия, отличающимися от привычным им. Отторжение вызывает также и специфический Интернет язык, часто отсылающих пользователей к терминологии, с которые пожилые, ввиду низких навыков информационной грамотности, незнакомы. Таким образом происходит формирование «чуждого» для пожилых людей пространства, что напрямую влияет на их доверие к провайдерам услуг, существующих в рамках подобного пространства. Повышение же степени доверия и обеспечение цифровой безопасности сервисов должно быть основано на принципах той социальной реальности (в особенности языка), к которой привыкли пожилые люди, и на учете их потребностей, для чего цифровым экосистемам и включенных в них сервисам следует проводить регулярный мониторинг. С точки зрения же политики цифровизации, необходимо содействовать развитию у пожилых людей не только навыков работы с устройством для выхода в Интернет, но и самими навыками взаимодействия с цифровым пространством. Понимание пожилыми людьми принципов обеспечения безопасности цифровых сервисов, основанное на объяснении данных принципов в пределах понятной терминологии, может способствовать росту доверия к пожилых не только к конкретным провайдерам, но и ко всему Интернет-пространству в целом.

Таким образом, обеспечение безопасности цифровых сервисов, ориентированных на пожилых пользователей, должно строиться не только на повышении объективных стандартов цифровой безопасности, но и повышении степени доверия пожилых людей к данным сервисам. Повысить доверие предполагается посредством обеспечения сервисов авторитетностью, которая может быть основана на взаимосвязи цифрового сервиса либо с традиционным институтом, либо с конкретной и знакомой пожилому человеку организацией. Другой возможный механизм повышения доверия к цифровым сервисам — создания благоприятной цифровой среды для пожилых пользователей, базирующейся на знакомых для них паттернах и принципах, в результате чего становится возможно нивелировать негативное влияние субъективного ощущения чуждости интернет-пространства, напрямую влияющего на степень доверия пожилых к цифровым сервисам.

Работа выполнена за счет гранта Российского научного фонда № 22-18-00461 «Отложенное старение или поздняя взрослость в России: как цифровое развитие меняет статус пожилых в эпоху COVID-19 и неопределенности» (https://rscf.ru/project/22-18-00461/).

СПИСОК ЛИТЕРАТУРЫ

1. World Population Ageing. 2020 Highlights: Living arrangements of older persons // Department of Economic and Social Affairs, Population Division. United Nations, 2022. P. 44.
2. Распределение населения в возрасте 15 лет и старше, являющегося активными пользователями сети Интернет, по возрастным группам, по субъектам Российской Федерации — 2021-2022 [Электронный ресурс] // стат. сб. / Фед. служба гос. стат. М: Росстат, 2021.URL: https://gks.ru/free_doc/new_site/business/it/ikt22/index.html (дата обращения: 09.04.2023).
3. Григорьева И.А., Петухова И.С. Интернет-практики пожилых: 10 лет развития и изучения // Государство и граждане в электронной среде. 2019. № 3. С. 78-90.

4. Папакостас А. Становление цивилизованной публичной сферы: Недоверие, доверие и коррупция. М.: ВЦИОМ, 2016. 224 с.
5. Видясова Л.А., Кривошапкина А.С. Доверие городским электронным сервисам в Петербурге: анализ возрастных групп // International Journal of Open Information Technologies. 2022. Т. 10, № 11. С. 70-74.
6. Веселов Ю.В. Доверие в цифровом обществе // Вестник Санкт-Петербургского университета. Социология. 2020. Т. 13. Вып. 2. С. 129–143.

УДК 351

РАЗРАБОТКА БАЗЫ ДАННЫХ ДЕСТРУКТИВНОГО КОНТЕНТА НА ОСНОВЕ ДАННЫХ ИЗ МЕССЕНДЖЕРОВ

Углова Анна Борисовна [1], Низомутдинов Борис Абдуллохонович [2]
[1] Российский государственный педагогический университет им. А. И. Герцена
наб. реки Мойки, 48, Санкт-Петербург, 191186, Россия
[2] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: anna.uglova@list.ru, boris@itmo.ru

Аннотация. В докладе представлены результаты сбора базы данных деструктивного контента из мессенджеров и поисковых систем. Актуальность и научная значимость создания базы данных обусловлена необходимостью получения систематизированных знаний о содержательном наполнении популярных информационных источников, отслеживании деструктивного контента и создания системы мониторинга психологической безопасности.

Ключевые слова: telegram; мессенджеры; парсинг; деструктивный контент.

DEVELOPMENT OF A DATABASE OF DESTRUCTIVE CONTENT BASED ON DATA FROM MESSENGERS

Uglova Anna[2], Nizomutdinov Boris[2]
[1] The Herzen State Pedagogical University of Russia
48 Moika River Emb., St. Petersburg, 191186, Russia
[2] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: anna.uglova@list.ru, boris@itmo.ru

Abstract. The report presents the results of collecting a database of destructive content from messengers and search engines. The relevance and scientific significance of creating a database is due to the need to obtain systematic knowledge about the content content of popular information sources, tracking destructive content and creating a psychological security monitoring system.

Keywords: telegram; messengers; parsing; destructive content.

В поисковых системах широко представлены справочные, образовательные, коммерческие, развлекательные ресурсы по различным проблемам. Так как не существует ограничений в публикации материалов, зачастую вместе с полезными данными пользователь получает еще и эмоционально нагруженную, деструктивную информацию, которая может негативно влиять на его психическое состояние [1].

Информация, представленная в социальных сетях и мессенджерах, может вызывать различные эмоциональные состояния. Новости о трагических событиях может вызывать депрессию, тревогу, аутоагрессивные реакции [2].

Информация может влиять на формирование убеждений и мнений. Представление о конкретной проблеме может измениться в зависимости от того, какую информацию человек получает. «Демонизация» саморазрушающего поведения, искажает представления о людях, страдающих от различных психических и психологических заболеваний, снижая их желание обращаться за помощью. В то же время «романтизация» аутоагрессии также меняет отношение молодежи к серьезности данной проблемы.

Также информация о деструктивном поведении может способствовать формированию стереотипов и предрассудков. В мессенджерах представлено достаточно много однобокой информации о саморазрушающем поведении, которая скорее запугивает пользователя, а также в большом объеме представлена информация с предвзятым, оценочным отношением к людям, с аутоагрессивным поведением. Обилие подобной информации может создавать негативные стереотипы и ограничивающие убеждения [3].

Не стоит забывать о влиянии деструктивной информации на поведение пользователей. В мессенджерах много деструктивного контента, описывающего способы аутоагрессии. Например, информация о способах самоубийства, может помочь человеку реализовать свои суицидальные намерения, что увеличивает риск для его здоровья.

В связи с вышесказанным актуальным становится изучение популярного контента для создания программ развития информационной компетенции и коммуникации, внедрения практик осознанного потребления информации.

Для автоматизированного поиска подобного контента необходимо обучить систему на тестовых данных. Для решения этой задачи нами был проанализирован контент более чем 100 каналов Telegram, по итогу которого

отобраны деструктивные посты. Дополнительно, мы расширили нашу базу поисковыми запросами пользователей. Для этого, с применением Yandex Wordstat API нами было составлено семантическое ядро запросов пользователей по острым темам.

Полученные эмпирические данные представляют большой интерес как для научных исследований, для коммерческих разработок, а также для управляющих структур, заинтересованных в создании систем мониторинга психологической безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Alam M. N., Noor O. O., Azizan A. Do social media influence altruistic and egoistic motivation and green purchase intention towards green products? An experimental investigation. Cleaner Engineering and Technology. 2023. Vol. 15. Pp. 100669.
2. Pfefferbaum B., Nitiéma P., Newman E. The association of mass trauma media contact with depression and anxiety: A meta-analytic review // Journal of Affective Disorders Reports. 2020. Vol. 3. Pp. 100063.
3. Balhar Y. P., Singh S., Yadav Z. Media reporting on deaths due to suicide attributed to gaming in digital news: A case of misrepresentation and missed opportunities // Asian Journal of Psychiatry. 2021. Vol. 68. Pp. 102955.

УДК 351

РОЛЕВАЯ МОДЕЛЬ ЭКОСИСТЕМЫ ГОРОДСКИХ СЕРВИСОВ: ИССЛЕДОВАНИЕ ПОТРЕБНОСТЕЙ БИЗНЕС-СФЕРЫ

Юпланов Марк Намикович
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: markyuplanov@gmail.com, markyuplanov@yandex.ru

Аннотация. Тезисы представляют обзор пилотного исследования, которое выявило связь между цифровыми сервисами и точками роста отношений между государственными институтами и малым и средним бизнесом на примере города Санкт-Петербурга. Результаты выражены в виде факторов развития инфраструктуры города: регулярный обмен информацией между МСБ и IT-посредником, агрегирующий данные от государственных институтов, выявлены первичные потребности представителей МСБ в рамках ролевой модели, позволяющие повысить доверие к инструментам онлайн-взаимодействия с властью.

Ключевые слова: цифровые сервисы; государственные электронные сервисы; взаимодействие бизнеса и власти; пилотное исследование; интервьюирование; ИТ-навыки; экосистема городских сервисов.

ROLE MODEL OF THE URBAN SERVICE ECOSYSTEM: BUSINESS NEEDS RESEARCH

Yuplanov Mark
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
E-mails: markyuplanov@gmail.com, markyuplanov@yandex.ru

Abstract. This article presents an overview of a pilot study that identified the connection between digital services and the points of growth in relationships between government institutions and small and medium-sized businesses, using the example of the city of Saint Petersburg. The results are expressed in the form of city infrastructure development factors: regular information exchange between SMEs and IT intermediaries aggregating data from government institutions, primary needs of SME representatives within the role model framework, enabling increased trust in online interaction tools with authorities.

Keywords: digital services; government electronic services; business-government interaction; pilot study; interviews; IT skills; urban service ecosystem.

Актуальность автоматизации и дигитализации малого и среднего бизнеса характеризуется изменениями стратегических векторов крупных компаний и монополистов IT-рынка в сторону предоставления услуг, связанных с использованием Big Data для выполнения рутинных задач и повышенный спрос бизнеса в закупке цифровых данных с целью мониторинга текущей ситуации на рынке, корректировки стратегических планов бизнеса, помощи по принятию управленческих решений и организации новых бизнес-процессов, повышающих эффективность текущих.

В докладе представлены результаты комплексного исследования, касающегося запросов к цифровым сервисам среди представителей бизнес-сообществ и ассоциаций на примере Санкт-Петербурга, а также влияния удовлетворенности от существующих сервисов на уровень эффективности бизнес-процессов компаний, включенных в данные бизнес-сообщества и ассоциации.

Влияние Интернета на действия малого и среднего бизнеса и повышение эффективности стоящих перед бизнесом задач представляет большой интерес для исследователей [1]. Анализ исследований и бизнес-планов по отраслям и рынкам экономики России от крупных агентств [2] показывает необходимость в дигитализации бизнеса для сохранения конкурентных позиций и обеспечения устойчивого развития бизнеса в краткосрочных и долгосрочных перспективах. Отечественные исследования выделяют уровень инновационной активности организаций по видам экономической деятельности: промышленное производство (17,4 %), сфера услуг (10,5 %), сельское хозяйство (8,1 %), строительство (4,5 %), обрабатывающие производства (23,1 %).

В период августа-сентября 2023 года было проведено пилотное исследование, интервьюирование представителей сегментов IT-бизнеса, услуг для населения, сельского хозяйства, туризма, HoReCa. Темы глубинного интервью затрагивали личный опыт взаимодействия с цифровыми сервисами, результаты интеграции цифровых сервисов и IT-решений в бизнес-процессы предприятия, опыта взаимодействия власти и бизнеса респондента и долгосрочные планы дальнейшей цифровизации бизнеса и использования информации, как инструмента помощи принятия управленческих решений, степень доверия к институтам и технологиям, оценка взаимодействия между малым и средним бизнесом и представителями в режиме онлайн [3].

Для оценки потребностей бизнес-сферы сформированы вопросы на темы текущего состояния бизнеса, влиянием цифровизации на бизнес-процессы, опытом использования систем автоматизации и сервисов сбора информации для нужд предприятия, видение будущего взаимодействия власти и бизнеса, оценка перспектив развития взаимодействия на примере платформы ЭГС. Данные унифицированы и обезличены по соображениям информационной безопасности и конфиденциальности данных. Исследование производилось на основе гипотезы о взаимосвязи между использованием цифровых сервисов, влиянием на эффективность управления предприятием и принятием управленческих решений, взглядах на текущую ситуацию взаимодействия между институтами.

Глубинное интервью проводилось через онлайн-сервис «Телемост» от компании Яндекс, участие приняли 15 респондентов из сфер среднего и малого бизнеса, микропредприятий. Время глубинного интервью ограничивалось 20 минутами каждый. Критериями отбора кандидатов на глубинное интервью являлось: опыт предпринимательской деятельности более 15 лет, подходящие под одну из вышеизложенных категорий бизнеса, имеющие опыт цифровизации и дигитализации бизнес-процессов, имеющие опыт взаимодействия с органами власти.

В процессе исследования были определены, какие IT-решения и сервисы используются при взаимодействии с органами власти. Преимущественно респонденты указали на IT-решение 1С-Fresh (86,6%) для взаимодействия с налоговыми органами, наименее используемое IT-решение — DSP на DOOH (13,3%) для сегментирования аудитории потребителей и целью распространения знания о бренде предприятия и товарной матрице. Так же были описаны текущие преимущества использования офлайн-каналов коммуникации с представителями органов власти при решении проблем.

Кроме этого, были выявлены потребности представителей предприятий в рамках роли ЭГС «Я предприниматель»:

– консультации с частными лицами в режиме онлайн (юридическая поддержка, нотариальные консультации и другие);

– автоматизация согласований с комитетами и органами власти, процессов получения разрешений и лицензий;

– мониторинг городской инфраструктуры в разрезах в виде «Тепловая карта» (для подбора помещений, подходящих под расширенные требования отделов развития компаний, проходящий трафик населения, социально-демографические характеристики жителей домов для размещения бизнеса);

– мониторинг запросов от населения к органам власти для выявления дополнительных потребностей жителей (ремонт, строительство, отходы, коммуникации, безопасность).

– исследование подтвердило гипотезу о взаимосвязи между использованием цифровых сервисов и уровнем эффективности предприятия, как инструмент благоприятного влияния на отношения представителей малого и среднего бизнеса с властью.

– Результаты глубинного интервью выявили несколько факторов, которые связаны с этой взаимосвязью:

– предоставление гарантий долгосрочной перспективы развития интеграции государственных онлайн сервисов в предприятие;

– организация прозрачной системы интересов всех стейкхолдеров процесса интеграции;

– уверенность в рассчитываемом результате внедрения сервисов, подтверждающего прогнозируемую выгоду предприятию;

– гарантии обезличивания данных и безопасности со стороны сервиса-посредника, обрабатывающего данные;

– возможность гибкой настройки получаемых данных и возможность интеграции с внутренними системами автоматизации бизнес-процессов предприятия;

– получение эксклюзивных данных от цифровых сервисов, которыми владеют государственные институты.

Другой выявленной в ходе исследования закономерностью является доверие к взаимодействию с органами власти через средства Интернет-технологий и уверенность в ускоренном решении задач при взаимодействии онлайн. Представители бизнеса с отсутствием теневых областей собственного бизнеса склонны доверять такому типу взаимодействия (73,3%), при условии, что гарантии сохранности и обезличивания данных будут подтверждены действиями по страхованию объектов информации, поскольку имеют убеждение в том, что информация может неверно шифроваться, а инструменты обезличивания информации могут быть некорректны, что может привести к проблемам юридического характера для бизнеса. Результаты интервью дают возможность изучить различия между подходом к взаимодействию бизнеса с органами власти в разрезе типов бизнеса и возможности организации теневой бухгалтерии в рамках бизнеса.

В будущем планируется разработать методологию многофакторной оценки потребностей бизнес-сферы. Эта методика будет использовать данные из количественного исследования, открытых исследований и других доступных источников, что позволит провести тестирование новых гипотез.

СПИСОК ЛИТЕРАТУРЫ

1. Индикаторы инновационной деятельности: 2023: статистический сборник / В.В. Власова, Л. М. Гохберг, Г.А. Грачева и др.; Нац. исслед. ун-т «Высшая школа экономики». М.: НИУ ВШЭ, 2023. 292 с. URL: https://issek.hse.ru/mirror/pubs/share/819414883.pdf (дата обращения: 01.09.2023).
2. Lola I., Bakeev M. Technology adoption expectations in the face of temporal uncertainty: an analysis of survey data from manufacturing firms // Technology Analysis & Strategic Management. 2021.
3. Лола И. С., Бакеев М. Б. Эффекты влияния экономико-технологического развития ИТ-сегмента на цифровую трансформацию розничной торговли // Вопросы статистики. 2019. Т. 26, № 11. С. 18-35.

.

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

УДК 004.896

ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ В ЗАДАЧЕ АВТОНОМНОЙ НАВИГАЦИИ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Беляев Павел Юрьевич, Зикратов Игорь Алексеевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mails: belyaev.edu@gmail.com, zikratov.ia@sut.ru

Аннотация. Рассматриваются основные методы автономной навигации беспилотных летательных аппаратов на основе нейронных сетей.

Ключевые слова: визуальная навигация; распознавание объекта; сверточные нейронные сети; БПЛА; сенсоры.

USAGE OF NEURAL NETWORKS IN THE SOLUTION OF AUTONOMOUS NAVIGATION OF UNMANNED AERIAL VEHICLES

Belyaev Pavel, Zikratov Igor
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: Belyaev.edu@gmail.com, zikratov.ia@sut.ru

Abstract. The main methods of autonomous navigation of unmanned aerial vehicles based on neural networks are considered.

Keywords: visual navigation; object detection; convolutional neural networks; UAVs; sensors.

В последнее время все больше внимания уделяется автономным робототехническим системам и беспилотным летательным аппаратам (БПЛА) в различных областях, включая исследования, разведку, мониторинг, доставку грузов и другие ресурсоемкие задачи. Одним из центральных вопросов, стоящих перед разработчиками таких систем, является создание эффективных методов навигации, позволяющих БПЛА безопасно и точно перемещаться в заданной области. В этом контексте визуальная навигация становится все более перспективным подходом, основанным на использовании визуальной информации для определения местоположения и ориентации БПЛА в окружающей среде. Современные сверточные нейронные сети, демонстрируя впечатляющую эффективность в обработке изображений, стимулируют исследователей к внедрению этой технологии в задачи визуальной навигации [1].

Использование методов оптической навигации БПЛА в сложной местности сопряжено со значительными техническими и вычислительными сложностями. Понимание сложной местности включает в себя разнообразные факторы, такие как нерегулярный рельеф, наличие препятствий, непостоянные условия освещения, ограниченная обзорность и видимость, а также непредсказуемые природные явления.

Оптическая навигация БПЛА на основе нейронных сетей представляет собой современный и эффективный подход, который использует глубокое обучение для анализа визуальной информации и определения местоположения, ориентации и движения БПЛА в окружающей среде. Основными методами навигации на основе БПЛА служат: методы на основе глубокого обучения [2, 3], семантическая сегментация [4-6], глубокое обучение для определения оптического потока [7, 8], обучение с подкреплением [9, 10]. Данные методы, основанные на использовании нейросетевых технологий, позволяют адаптировать задачи автономной навигации под различные сложные условия.

Применение методов на основе глубокого обучения используется для классификации объектов и окружения с БПЛА, что позволяет БПЛА определять свою позицию относительно опознанных объектов и ориентироваться в среде. Методы семантической сегментации позволяют сегментировать изображение на различные классы объектов и поверхности, что позволяет БПЛА более точно анализировать окружающую среду и определять свою позицию относительно различных областей. Методы оптического потока направлены на анализ парных изображений, полученных с различных камер, и позволяют определять глубину и расстояние до объектов на основе разницы в изображениях, что способствует определению

положению БПЛА в пространстве. Обучение с подкреплением направлено на отработку различных стратегий поведения БПЛА в изменяющейся среде функционирования.

Таким образом, нейронные сети могут быть эффективно использованы для автономной навигации БПЛА во всех основных элементах системы.

СПИСОК ЛИТЕРАТУРЫ

1. Object detection in optical remote sensing images: A survey and a new benchmark / Li K. [et al] // ISPRS journal of photogrammetry and remote sensing. 2020. Vol. 159. Pp. 296-307.
2. Kaluthantrige A., Feng J., Gil-Fernández J. CNN-based Image Processing algorithm for autonomous optical navigation of Hera mission to the binary asteroid Didymos //Acta Astronautica. 2023. Vol. 211. C. 60-75.
3. Autonomous UAV trail navigation with obstacle avoidance using deep neural networks / Back S. [et al] // Journal of Intelligent & Robotic Systems. 2020. Vol. 100. Pp. 1195-1211.
4. Motion and depth augmented semantic segmentation for autonomous navigation / Rashed H. [et al] // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops. 2019.
5. Scene terrain classification for autonomous vehicle navigation based on semantic segmentation method / Julius Fusic S. [et al] // Transactions of the Institute of Measurement and Control. 2022. Vol. 44. №. 13. Pp. 2574-2587.
6. Improved real-time semantic segmentation network model for crop vision navigation line detection / Cao M. [et al] // Frontiers in Plant Science. 2022. Vol. 13. Articles 898131.
7. An improved optical flow algorithm based on mask-R-CNN and K-means for velocity calculation / Peng Y. [et al] // Applied Sciences. 2019. Vol. 9. №. 14. Articles 2808.
8. Mumuni F., Mumuni A., Amuzuvi C. K. Deep learning of monocular depth, optical flow and ego-motion with geometric guidance for UAV navigation in dynamic environments // Machine Learning with Applications. 2022. Vol. 10. Articles 100416.
9. Drone deep reinforcement learning: A review / Azar A. T. [et al] // Electronics. 2021. Vol. 10. №. 9. Articles 999.
10. AlMahamid F., Grolinger K. Autonomous unmanned aerial vehicle navigation using reinforcement learning: A systematic review // Engineering Applications of Artificial Intelligence. 2022. Vol. 115. Articles 105321.

УДК 004.946

СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЦИФРОВЫХ ДВОЙНИКОВ ПРОСТРАНСТВЕННЫХ ОБЪЕКТОВ

Верхова Галина Викторовна, Акимов Сергей Викторович,
Прощенков Валерий Михайлович, Юрчик Даниил Сергеевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: galina500@inbox.ru, akimov-sv@yandex.ru, valery@proshchenkov.ru, urdanyrec@yandex.ru

Аннотация. Представлены результаты исследований в области цифровых двойников пространственно-распределенных объектов. Рассмотрены современное состояние цифровых двойников пространственных объектов и перспективы развития. Показано, что эффективное построение цифровых двойников возможно лишь на базе многоаспектных геоинформационных моделей, в которых выполнен синтез общесистемных и геоинформационных объектов.

Ключевые слова: цифровой двойник; пространственный объект; многоаспектные геоинформационные модели; общесистемные аспекты; географические аспекты; комплексные модели.

CURRENT STATE AND PROSPECTS FOR THE DEVELOPMENT OF DIGITAL TWINS OF SPATIAL OBJECTS

Verhova Galina, Akimov Sergei, Proshchenkov Valerii, Iurchik Daniil
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
22 Bol'shevikov Av, St. Petersburg, 193232, Russia
e-mails: e-mails: galina500@inbox.ru, akimov-sv@yandex.ru, valery@proshchenkov.ru, urdanyrec@yandex.ru

Abstract. The results of research in the field of digital twins of spatially distributed objects are presented. The current state of digital twins of spatial objects and development prospects are considered. It is shown that the effective construction of digital twins is possible only on the basis of multidimensional geoinformation models, in which the synthesis of system-wide and geoinformation objects is performed.

Keywords: digital twin; spatial object; multidimensional geoinformation models; system-wide aspects; geographical aspects; complex models.

Геоинформационные технологии нашли широкое применение во всех сферах человеческой деятельности [1]. В условиях глобальной цифровой трансформации всех отраслей и видов деятельности необходимо создание единого информационного пространства, в котором географические аспекты будут синтезированы вместе с общесистемными аспектами. Технология цифровых двойников является наиболее перспективной для решения различных задач, связанных с применением геоинформационных технологий [2-3]. Цифровой двойник позволяет создать наиболее адекватное представление объекта в виртуальном пространстве, которое может быть синхронизирован в реальном времени с помощью применения системы сенсоров.

Интеграций гетерогенной информации о пространственно-распределенном объекте в рамках цифрового двойника является сложной задаче, решение которой может быть эффективно выполнено лишь на базе

многоаспектных моделей — комплексных и интегративных [4-5], которые позволяют интегрировать общесистемные и географические аспекты в единую модель. Многоаспектные геоинформационные модели позволят создавать цифровые 5D-двойники, которые позволят создать единое киберфизическое пространство постиндустриального общества.

Проект реализуется победителем грантового конкурса для преподавателей магистратуры 2021/2022 Стипендиальной программы Владимира Потанина.

СПИСОК ЛИТЕРАТУРЫ

1. Карпик А. П. Методологические и технологические основы геоинформационного обеспечения территорий : монография. Новосибирск: СГГА, 2004. 259 с.
2. Акинина Н. В., Курагин А. В., Колесенков А. Н., Костров Б. В. Разработка картографических веб-приложений на основе геоинформационных технологий // Телекоммуникации. 2023. № 2. С. 23-31.
3. Харламов С. Ю. Цифровой двойник как элемент применения ГИС-технологий в развитии территории // Пространственное развитие территорий. III Международная научно-практическая конференция: сборник научных трудов / под общей ред. Е. А. Стрябковой, А. М. Кулик. Б., 2020. С. 189-192.
4. Кходер Х., Верхова Г. В., Акимов С. В. Модульная технология проектирования гибких сложных систем // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 9. С. 86-90.
5. Акимов С. В., Меткин Н. П. Архитектура среды многоаспектного моделирования для автоматизации решения задач исследования, проектирования и управления // Вопросы радиоэлектроники. 2013. Т. 1. № 1. С. 32-40.

УДК 004.056.55

ИССЛЕДОВАНИЕ И РАЗРАБОТКА АЛГОРИТМОВ ДИНАМИЧЕСКОЙ СТЕГАНОГРАФИИ ДЛЯ ГРАФИЧЕСКИХ КОНТЕЙНЕРОВ

Волынкин Павел Александрович, Гибадуллин Альберт Артурович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Мойки р. наб, 61, лит. А, Санкт-Петербург, 191186, Россия
e-mails: pavelas@mail.ru, theelementoffire@mail.ru

Аннотация. Рассматриваются методы и средства стеганографии для графических контейнеров. Исследованы возможности разработки алгоритмов и создания программного обеспечения для средств мобильной связи, позволяющее проводить исследования эффективности оперативного внедрения контента в графические контейнеры.

Ключевые слова: стеганография; графические контейнеры; LSB-алгоритмы; экспертные оценки; цветовой фон контейнера.

RESEARCH AND DEVELOPMENT OF DYNAMIC STEGANOGRAPHY ALGORITHMS FOR GRAPHIC CONTAINERS

Volynkin Pavel, Gibadullin Albert
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
61Moika Emb, letter A, St. Petersburg, 191186, Russia
e-mails: pavelas@mail.ru, theelementoffire@mail.ru

Abstract. The methods and means of steganography for graphic containers are considered. Possibilities of developing algorithms and creating software for mobile communications, allowing to conduct research on the effectiveness of the rapid implementation of content in graphic containers, have been explored.

Keywords: steganography; graphics containers; LSB algorithms; expert assessments; color background of the container.

В стеганографии с использованием графических контейнеров скрываемый контент желательно размещать в контейнере с максимальной плотностью, но не в ущерб конфиденциальности.

Многообразие стеганографических контейнеров включает в себя различные типы файлов, которые могут быть использованы в качестве контейнеров для скрытой информации.

Некоторые из наиболее распространенных типов контейнеров включают в себя: JPEG, BMP, PNG, GIF, TIFF и другие форматы изображений могут быть использованы в качестве контейнеров для скрытой информации.

Ставится задача разработки алгоритма и программного обеспечения для мобильных устройств с последующей целью исследования эффективности максимального использования битов для LSB-алгоритмов стеганографии.

Для решения данной задачи разработано мобильное приложение, позволяющее выбирать различные графические контейнеры. После загрузки контейнера программа оценивает средний цветовой фон контейнера. Кроме этого, приложение позволяет управлять (включать или отключать) любыми битами для каждого из трех RGB-каналов с целью внедрения в эти биты содержимого скрываемого контента. Эта функция должна дать возможность пользователю формировать любые сочетания битов для каждого из трех цветовых каналов. Подобные сочетания в свою очередь могут создавать цветовые фильтры, которые должны как выключать определенные биты из контейнера, так и внедрять в эти биты скрываемую информацию.

СПИСОК ЛИТЕРАТУРЫ

1. Волынкин П. А., Севостьянова А. С. Исследование принципов шифрования мультимедиа информации в графических файлах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. Т. 2. 2018. С. 203–206.
2. Волынкин П. А., Кононюк О. А. Исследование стеганографического метода LSB с использованием ключей для определения области встраивания данных в графических контейнерах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). Сборник научных статей IX Международной научно-технической и научно-методической конференции. В 4-х т. Санкт-Петербург, 2020. С. 186-190.
3. Волынкин П. А., Кононюк О. А. Исследование стеганографического метода LSB с адаптивным поиском областей встраивания данных в растровых графических контейнерах. // Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей: в 4-х т. Санкт-Петербург, 2021. С. 159-163.

УДК 004.934

РАЗРАБОТКА МЕТОДИКИ, АЛГОРИТМИЧЕСКОГО И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОЦЕНКИ КАЧЕСТВА ШИФРОВАНИЯ

Волынкин Павел Александрович, Кузнецов Вадим Всеволодович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Мойки реки наб., 61, лит. А, Санкт-Петербург, 191186, Россия
e-mails: pavelas@mail.ru, vadim.kuznetsov.2001@gmail.com

Аннотация. Рассматриваются методы и средства криптографии. Исследованы существующие и предложены авторские алгоритмы для реализации программного обеспечения по оценке качества криптографических методов.

Ключевые слова: криптография; алгоритм; программное обеспечение; качество шифрования.

DEVELOPMENT OF METHODS, ALGORITHMIC AND SOFTWARE FOR ASSESSING THE QUALITY OF ENCRYPTION CONTAINERS

Volynkin Pavel, Kuznetsov Vadim
The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
61 Moiki Emb, lit. A., St. Petersburg, 191186, Russia
e-mails: pavelas@mail.ru, vadim.kuznetsov.2001@gmail.com

Abstract. Methods and means of cryptography are considered. Existing algorithms for the implementation of software for assessing the quality of cryptographic methods are investigated and author's algorithms are proposed.

Keywords: cryptography; algorithm; software; encryption quality.

В криптографии существует огромное количество методов и методик шифрования передаваемой информации. Ставится задача разработки методов, алгоритмов и программного обеспечения для комплексной оценки качества тех или иных методов шифрования.

Существует множество криптографических алгоритмов, каждый из которых имеет свои уникальные характеристики и стойкость. Однако, не все алгоритмы обладают одинаковой стойкостью к атакам и возможностью обнаружения. Поэтому важно разработать методику, которая позволит анализировать криптографические алгоритмы с целью определения их качества и стойкости.

Предлагается использовать такие показатели как: байтовую энтропию, дисперсию n-грамм и битовые карты, для анализа криптографических алгоритмов.

Байтовая энтропия является мерой неопределенности информации и может быть рассчитана на основе распределения байтов в зашифрованных данных. Высокое значение энтропии указывает на хорошую случайность данных и стойкость алгоритма.

Дисперсия n-грамм представляет собой меру изменчивости последовательности n-грамм в зашифрованных данных. Большая дисперсия указывает на равномерное распределение n-грамм и отсутствие явных паттернов, что также является признаком стойкости алгоритма.

Битовые карты позволяют визуально представить изменения в паттернах данных после применения алгоритма шифрования. Битовые карты представляют собой графическое изображение, где каждый пиксель соответствует одному биту данных. После шифрования можно сравнить битовые карты и определить, сохраняются ли паттерны или происходят значительные изменения.

Анализ с помощью битовых карт дает дополнительную информацию о влиянии алгоритма на данные. Если после шифрования паттерны остаются неизменными, это может указывать на недостаточную стойкость алгоритма и возможность восстановления исходной информации. С другой стороны, если паттерны полностью меняются или становятся случайными, это может свидетельствовать о хорошей стойкости алгоритма и невозможности восстановления данных без правильного ключа.

Использование битовых карт в сочетании с байтовой энтропией и дисперсией n-грамм позволяет получить более полное представление о криптографическом алгоритме, его стойкости и воздействии на данные.

Такой комплексный анализ способствует более точному и надежному оцениванию качества и безопасности алгоритмов шифрования. Разработаны алгоритмы и программное обеспечение для реализации вышеописанных методик.

СПИСОК ЛИТЕРАТУРЫ

1. Зарипов Р. Г. Новые меры и методы в теории информации. К. : Казанский государственный технический университет, 2005. 364 с.
2. Кац Дж., Линделл Ю. Введение в современную криптографию. CRC Press, 2014. 598 с.
3. Лавасани А., Эглидос Т. Практический тест следующего бита для оценки псевдослучайной последовательности // Научный журнал Scientia Iranica. 2009. Т. 16. Вып. 1. Серийный номер 1.
4. Сен Н. Д., Котляров В. П., Григорьев Я. Ю., Применение оценок на основе энтропии для сравнения криптостойкости алгоритмов шифрования // Современные наукоемкие технологи. 2013. № 2. С. 105-106.

УДК 004.056

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ТЕХНОЛОГИИ OWE В БЕСПРОВОДНОЙ СЕТИ СО СТАНДАРТОМ WPA3

Герлинг Екатерина Юрьевна, Зебзеев Егор Алексеевич, Кируга Антон Юрьевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mails: zebzeev.avis@gmail.com, gerlingeu@gmail.com, anton.kistruga@gmail.com

Аннотация. В работе рассматриваются особенности обеспечения информационной безопасности стандарта WPA3. Подробно описан механизм OWE, являющийся одним из ключевых новшеств WPA3. А также представлены сложности, встречающиеся при внедрении этого механизма в WLAN сетях.

Ключевые слова: WPA3; SAE; OWE; информационная безопасность.

SPECIFICITY OF ANALYSIS OF WLAN TRAFFIC WITH WPA2-ENTERPRISE STANDART

Gerling Ekaterina, Zebzeev Egor, Kistruga Anton
Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
22 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: zebzeev.avis@gmail.com, maxkovzur@mail.ru, gerlingeu@gmail.com, anton.kistruga@gmail.com

Abstract. The paper discusses the features of the ensuring information security of the WPA3 standard. The OLE mechanism is described in detail. The difficulties of the implementation of this mechanism in WLAN networks are presented.

Keywords: WPA3; SAE; OWE; information security.

Безопасности передачи данных всегда уделяется отдельное внимание, особенно в беспроводных сетях. Это связано с тем, что среда передачи является открытой, а передаваться могут, как персональные данные отдельного пользователя, так и конфиденциальная информация компании [1]. Актуальным стандартом безопасности Wi-Fi сетей является Wi-Fi Protected Access 3. В сертифицированных устройствах Wi-Fi 5 данный стандарт не является обязательным, но для Wi-Fi 6 он является нативным. Следовательно, к безопасности современных WLAN стоит подходить с приоритетом использования данного стандарта [2].

По сравнению с предыдущим стандартом WPA3 имеет следующие основные особенности:

– Opportunistic Wireless Encryption (OWE);
– Simultaneous Authentication of Equals (SAE);
– 192-бит шифрование (опционально);
– Easy Connect (Device Provisioning Protocol, замена WPS) [3].
– OWE — это технология, призванная главным образом заменить уязвимый режим предварительного доступа с общим ключом (PSK) [4].

PSK используется в процессе четырехстороннего рукопожатия, в котором устройства вырабатывают ключи шифрования трафика. Основная проблема заключается в том, что, зная PSK и перехватив четырехстороннее рукопожатие, злоумышленник может самостоятельно вычислить ключи шифрования. Главной особенностью WPA3 является способность противостоять атакам по офлайн словарю на пароль сети Wi-Fi [5]. В WPA2 использовалась аутентификация с предустановленным ключом PSK, при которой для клиента и точки доступа формировался общий PMK (Pairwise Master Key).

При OWE клиент и точка доступа (ТД) используют протокол обмена ключами Диффи-Хеллмана и получают общий секрет вместо PSK.

Основная идея — это передача открытых ключей Диффи-Хеллмана в сообщениях Assoc Req и Assoc Reg, после чего происходит выработка общего секрета, который используется при вычислении ключей шифрования.

Использование OWE обеспечивает защиту от атаки типа «MITM», а также позволяет защитить фреймы управления, но из-за того, что протокол не предусматривает аутентификацию ТД, имеется уязвимость перед атаками типа Honeypot и Evil Twin AP [6].

В работе подробно рассмотрен процесс генерации общего секрета при использовании механизма OWE. Также рассмотрены основные сложности использования стандарта WPA3 в WLAN сетях.

СПИСОК ЛИТЕРАТУРЫ

1. Дешевых Е. А., Конюхов В. М., Крылов К. Ю., Ушаков И. А. Исследование методов защиты от инсайдерских атак // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция : сб. научных статей в 2 т. 2015. С. 310-313.
2. Kovtsur M., Minyaev A., Khramtsov D., Abramenko G. Investigation of attacks and methods of protection of wireless networks during authorization using the IEEE 802.1X protocol // ACM International Conference Proceeding. Series. 5. The Premier Conference on Smart Next Generation Networking Technologies. ICFNDS 2021 — 5th International Conference on Future Networks and Distributed Systems: The Premier Conference on Smart Next Generation Networking Technologies, 2021. С. 555-561.
3. WPA3 Specification Version 3.1 // Wi-FI Alliance. 2019.
4. RFC 8110. Opportunistic Wireless Encryption, 2017.
5. Герлинг Е. Ю., Зебзеев Е. А., Казаков Н. И., Ковцур М. М. Разработка метода анализа wlan трафика в сетях с WPA2 ENTERPRISE // Региональная информатика и информационная безопасность: сб. трудов Юбилейной XVIII Санкт-Петербургской международной конференции. Санкт-Петербург, 2022. С. 575-578.
6. Юркин Д. Ю., Ворошнин Г. Е., Ковцур М. М., Мисливский Б. С. Исследование влияния атак arpinject и associationflood в беспроводных сетях на базе оборудования MIKROTIK // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. № 1. С. 44-48.

УДК 519.6

ИССЛЕДОВАНИЕ ИНФОРМАЦИОННОЙ МОДЕЛИ ОЦЕНКИ УРОВНЯ ПОДГОТОВКИ СТУДЕНТОВ ПРИ ТЕСТИРОВАНИИ

Губин Александр Николаевич, Михайлова Екатерина Александровна
Санкт-Петербургский государственный университет телекоммуникаций им. Проф. М. А. Бонч-Бруевича,
Большевиков пр., 22, Санкт-Петербург, 193232, Россия
e-mails: gan50_60@mail.ru, kate200197@gmail.com

Аннотация. Рассматриваются модели оценивания знаний студентов при тестировании, а также влияние уровня стресса на результат тестирования.

Ключевые слова: тестирование; классическая модель; модель с учетом времени выполнения заданий; модель на основе уровней; модель Раша; модель Бирнбаума.

RESEARCH ON INFORMATION MODEL FOR ASSESSING STUDENT LEARNING LEVELS IN TESTING

Gubin Alexander, Mikhaylova Ekaterina
St. Petersburg State University of Telecommunications in Saint-Petersburg. M.A. Bonch-Bruevich
St. Petersburg State University of Telecommunications
22 Bolsheviks Av, St. Petersburg, 193232, Russia
e-mails: gan50_60@mail.ru, kate200197@gmail.com

Abstract. This article deals with models of knowledge estimation in testing as well as with influence of stress level on testing results.

Keywords: testing; classical model; time-based model; level-based model; Rasch model; Birnbaum model.

По мере развития информационных технологий обычная форма контроля освоения учебного материала частично заменяется проведением тестирования. Особенно, проведение тестовых заданий широко распространено в формате дистанционного обучения.

Для того чтобы наиболее объективно оценить качество уровня подготовки студентов посредством тестирования, разработаны различные модели оценки знаний. В работе будут рассмотрены наиболее распространенные модели оценки знаний при тестировании.

Классическая модель является самой простой моделью оценивания знаний. В данной модели ответы оцениваются по двухбалльной (правильно или неправильно) или многобалльной (например, пятибалльной) шкале. В настоящее время происходит уход от использования данной модели к более совершенным и эффективным моделям [1].

В моделях, учитывающей время выполнения задания при определении результата учитывается время ответа на каждое задание или на весь тест. Этот метод позволяет определить, насколько самостоятельно выполняется тестирование. В случае, если студент не обладает достаточными знаниями для успешного прохождения теста, он потратит много времени на поиск ответов в сторонних источниках и не успеет ответить на все вопросы. Модель, учитывающая время выполнения задания, используется в Братском государственном техническом университете [2].

В модели на основе уровней усвоения характеристикой усвоения учебного материала является уровень. Уровни разделяются на следующие группы: понимание, опознание, воспроизведение, применение и творческая деятельность. Задания составляются для каждого из пяти уровней, при этом переход на следующий уровень

возможен только в случае успешного освоения предыдущего. Модель на основе уровней усвоения используется в системе КАДИС [3].

В рамках современной теории тестов разработаны три логистические модели, которые различаются числом задействованных параметров: однопараметрическая модель Раша, двухпараметрическая и трехпараметрическая модели Бирнбаума. Дополнительные параметры каждой модели влияют на применимость и получаемую по итогам анализа информацию. В рамках данных моделей параметры – это переменные, не подлежащие непосредственному измерению (латентные переменные). Все параметры измеряются через испытуемых на тестовые задания. Логистические модели успешно применяются и в настоящее время в АОС ВУЗ [4].

Тестовые задания, составленные в целом по всему объему учебной дисциплины, дают возможность получить обобщенный срез знаний по всем аспектам и темам изученного курса, в то время как в традиционной системе проверки знаний студентов по экзаменационным билетам присутствует элемент случайности, выборочности (как правило, билет ограничивается 2-мя вопросами). При проведении тестирования, появляется возможность автоматизировать процесс оценки усвоения знаний студентом.

С помощью анализа результатов тестирования, можно выявить наиболее типичные ошибки, провести соответствующую работу по их исправлению, при необходимости корректировать учебный план.

В рассмотренных моделях отсутствует параметр стресса испытуемого во время прохождения тестирования, который также может влиять на результат.

В работе «Математическое моделирование психофизиологических факторов успешности обучения студентов первого курса медицинского вуза по дисциплине биофизика» проведено исследование, в результате которого, построена математическая модель зависимости балла, полученного за освоение дисциплины от таких факторов, как межэкзаменационный период, уровень интеллекта и частота сердцебиения [5].

С учетом математической модели зависимости балла от уровня стресса и трехпараметрической модели Бирнбаума, появляется возможность модифицировать модели таким образом, чтобы при прогнозировании результата тестирования, учитывались не только такие параметры как уровень подготовки испытуемого, сложность задания и дифференцирующая способность тестового задания, но и параметры, влияющие на уровень стресса. В результате, полученная модель позволит наиболее точно определять приблизительный результат успешной сдачи теста студентом.

СПИСОК ЛИТЕРАТУРЫ

1. Зайцева Л. В., Прокофьева Н. О. Модели и методы адаптивного контроля знаний // Образовательные технологии и общество. 2004. Т. 7. № 4. С. 265-277.
2. Соловов А. В. Проектирование компьютерных систем учебного назначения. С. : Самарский национальный исследовательский университет имени академика С. П. Королева, 1995. 138 с.
3. Бутина Т.Д. Модели оценки качества тестов в современной теории тестирования // Наука настоящего и будущего. 2020. Т. 2. С. 184-186.
4. Маслак А. А. Теория и практика измерения латентных переменных в образовании : монография. М. : Юрайт, 2022. 255 с.
5. Математическое моделирование психофизиологических факторов успешности обучения студентов первого курса медицинского вуза по дисциплине «биофизика» / Н. И. Колосова [и др.]. // Молодой ученый. 2017. № 22 (156). С. 168-170

УДК 004.056.53

ОБНАРУЖЕНИЕ АТАКИ НА TDLS БЕСПРОВОДНОГО УСТРОЙСТВА

Дрепа Владислав Евгеньевич, Ковцур Максим Михайлович,
Сахаров Дмитрий Владимирович, Шарапов Роман Игоревич
Санкт-Петербургский государственный университет телекоммуникаций им.проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп.1, лит. А, Ж, Санкт-Петербург, 193232, Россия
e-mails: vladikdrepa@mail.ru, maxkovzur@mail.ru, sguard7@mail.ru, sharapov.roman@list.ru

Аннотация. Рассматривается метод обнаружения атак на TDLS (Tunneled Direct Link Setup) чипсетов Broadcom — одного из крупнейших поставщиков чипсетов для беспроводных устройств. Уязвимости данных чипов могут стать катализатором кибератак и утечек данных, поэтому важно на ранних стадиях обнаруживать подобные инциденты и принимать меры по их предотвращению.

Ключевые слова: аппаратные уязвимости WLAN чипсетов; исследование чипсетов; Wi-Fi exploit; Broadcom; прошивка; reverse-engineering; TDLS.

ATTACK DETECTION ON TDLS WIRELESS DEVICE

Drepa Vladislav, Kovtsur Maxim, Sakharov Dmitry, Sharapov Roman
The Bonch-Bruevich St Petersburg State University of Telecommunications
22 Bolshevikov Av, bld 1, St. Petersburg, 193232, Russia
e-mails: vladikdrepa@mail.ru, maxkovzur@mail.ru, sguard7@mail.ru, sharapov.roman@list.ru

Abstract. A method for detecting TDLS (Tunneled Direct Link Setup) attacks on Broadcom chipsets, one of the largest suppliers of chipsets for wireless devices, is discussed. Vulnerabilities in these chips can become a catalyst for cyberattacks and data leaks, so it is important to detect such incidents at an early stage and take measures to prevent them.

Keywords: WLAN chipset hardware vulnerabilities; chipset research; Wi-Fi exploit; Broadcom; firmware; reverse-engineering; TDLS.

Атака на TDLS подразумевает перехват и изменение третьего пакета четырёхэтапного рукопожатия. В процессе обмена сообщениями точка доступа не выполняет проверку длины поля «WPA Key Data». Обнаружение манипуляций с полем «WPA Key Data» включает несколько технических шагов, связанных с мониторингом и анализом Wi-Fi трафика [1-5]. Ниже приведён базовый процесс обнаружения подобной атаки:

1. Первым шагом является подготовка всего необходимого оборудования. Потребуется компьютер, на котором установлена операционная система, поддерживающая мониторинг трафика Wi-Fi, например Kali Linux. Также потребуется Wi-Fi адаптер, поддерживающий режим мониторинга сети, например D-Link DWL-G122.

2. Перевод адаптера в режим мониторинга сети. В данном режиме Wi-Fi адаптер способен прослушивать и записывать все передаваемые пакеты данных, даже если они не предназначены для него.

3. Запись дампа сети. Для этой цели можно использовать инструменты, такие как Aircrack-ng, Wireshark или tcpdump. Рекомендуется использовать последний, поскольку он не требует значительных ресурсов процессора.

4. Анализ пакетов. Wireshark — один из лучших инструментов для анализа сетевого трафика. Для поиска пакетов, соответствующих третьему этапу четырёхэтапного рукопожатия и имеющих длину поля «WPA Key Data» больше допустимого значения, следует применить фильтр «(wlan_rsna_eapol.keydes.msgnr == 3) && (wlan_rsna_eapol.keydes.data_len > 63)».

5. Обнаружение подозрительных пакетов. Если поле «WPA Key Data» не соответствует ожидаемым значениям, например, если ключ шифрования кажется необычно длинным, превышает максимальное значение в 63 байта или содержит подозрительные данные, это может указывать на его изменение злоумышленником.

СПИСОК ЛИТЕРАТУРЫ

1. Reverse-engineering Broadcom wireless chipset // Quarkslab's blog [Электронный ресурс]. URL: https://blog.quarkslab.com/reverse-engineering-broadcom-wireless-chipsets.html (дата обращения: 02.02.2023).
2. Over The Air — Vol. 2, Pt. 1: Exploiting The Wi-Fi Stack on Apple Devices // Project Zero [Электронный ресурс]. URL: https://googleprojectzero.blogspot.com/2017/09/over-air-vol-2-pt-1-exploiting-wi-fi.html (дата обращения: 05.02.2023).
3. Сахаров Д. В., Красов А. В., Ушаков И. А., Бирих Э. В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPV6 // Защита информации. Инсайд. 2020 № 1 (91). С. 51-57.
4. Кистуга А. Ю., Ковцур М. М., Петров М. П., Шабанов В. П. Методика обнаружения местоположения нарушителя, реализующего атаку деаутентификации на сеть IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция. Т. 1 : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022. С. 561-564.
5. Ковцур М. М., Герлинг Е. Ю., Коновалова В. В., Кистуга А. Ю. Исследование способов удаленного перехвата трафика в корпоративных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2021. № 4. С. 68-75.

УДК 004.056

НОВЫЙ ПОДХОД К ИССЛЕДОВАНИЮ ЦЕЛОСТНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX В ПРОЦЕССЕ ЕЕ РАБОТЫ

Коньков Владимир Владимирович, Кузнецов Владимир Александрович, Красов Андрей Владимирович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков просп., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: No0boT2001@mail.ru, kuznetsov_v2001@mail.ru, krasov@inbox.ru

Аннотация. Данная статья представляет новый подход к исследованию целостности операционной системы Linux в процессе её работы. Операционная система Linux широко используется в различных сферах, и обеспечение её надежности и безопасности является критически важной задачей. В статье рассматриваются современные методы мониторинга и анализа, позволяющие более эффективно выявлять потенциальные угрозы и нарушения целостности в работе операционной системы Linux в реальном времени. Представляются инновационные технологии и инструменты, основанные на анализе системных журналов, системных вызовов, и многих других аспектах работы Linux. Разработанный подход позволяет оперативно обнаруживать аномалии, атаки и несанкционированные изменения в ядре операционной системы, что способствует повышению уровня безопасности и надежности Linux-систем. Исследование также описывает результаты экспериментов, проведенных на реальных системах, демонстрируя эффективность предложенного метода. Этот новый подход к исследованию целостности операционной системы Linux может быть весьма полезным для администраторов, разработчиков и специалистов по информационной безопасности, стремящихся обеспечить стабильную и защищенную работу Linux-систем в условиях современных угроз и вызовов.

Ключевые слова: C++; ОС Linux; внедрение; целостность; эффективность.

INVESTIGATION OF NEW APPROACH TO INVESTIGATING THE INTEGRITY OF THE LINUX OPERATING SYSTEM DURING ITS OPERATION

Konkov Vladimir, Kuznetsov Vladimir, Krasov Andrey
St. Petersburg State University of Telecommunications named after Professor M. A. Bonch-Bruevich
22 Bolshevikov Av, bld 1, St. Petersburg, 193232, Russia
e-mails: No0boT2001@mail.ru, kuznetsov_v2001@mail.ru, krasov@inbox.ru

Abstract. This article presents a novel approach to investigating the integrity of the Linux operating system during its operation. Linux is widely used in various domains, and ensuring its reliability and security is a critically important task. The article explores modern monitoring and analysis methods that allow for more effective detection of potential threats and integrity violations in the operation of the Linux operating system in real-time. Innovative technologies and tools based on the analysis of system logs, system calls, and many other aspects of Linux operation are introduced. The developed approach enables the timely detection of anomalies, attacks, and unauthorized changes in the kernel of the operating system, contributing to the enhancement of security and reliability of Linux systems. The research also describes the results of experiments conducted on real systems, demonstrating the effectiveness of the proposed method. This new approach to investigating the integrity of the Linux operating system can be highly valuable for administrators, developers, and information security professionals seeking to ensure stable and secure operation of Linux systems in the face of modern threats and challenges.

Keywords: C++; Linux OS; deployment; integrity; efficiency.

Операционная система Linux является фундаментальным элементом множества информационных систем, от веб-серверов до встраиваемых устройств. Её надежность и безопасность играют решающую роль в обеспечении стабильной работы множества приложений и сетей. В связи с этим, мониторинг и обеспечение целостности Linux-системы стали приоритетной задачей для администраторов, разработчиков и специалистов по информационной безопасности.

Существует множество методов и инструментов для исследования целостности операционной системы Linux. Современные методы проверки целостности операционной системы можно разделить на несколько категорий, каждая из которых использует различные подходы и технологии:

1. Контрольные суммы и хеширование: Этот подход включает в себя вычисление контрольных сумм или хэш-значений для важных системных файлов и их сравнение с заранее сохраненными значениями.

2. Цифровые подписи: Этот подход расширяет концепцию контрольных сумм и хеширования, добавляя дополнительный уровень защиты с помощью криптографии. Системные файлы и программы подписываются цифровыми сертификатами, которые можно проверить на аутентичность

Однако, на протяжении многих лет, эти методы имели свои ограничения и недостатки. Рассмотрим некоторые из них и обсудим, почему новый подход выделяется и превосходит их важными аспектами. Данный метод внедрения цифрового водяного знака основан на анализе и модификации некоторых секций ELF файла, связанных с кодом ядра. В процессе компиляции и сборки модуля ядра, мы встраиваем уникальный цифровой водяной знак, который содержит информацию о подлинности и идентификации кода. Этот метод позволяет защитить ядро от несанкционированных изменений и улучшить обнаружение поддельных или модифицированных версий кода. Это обеспечивает защиту от несанкционированных изменений и подделок, которые могут представлять угрозу безопасности системы.

Для дополнительной защиты целостности операционной системы Linux в процессе её работы, мы предлагаем инновационный метод внедрения цифрового водяного знака. Метод основан на анализе и модификации определенных секций ELF-файла, связанных с кодом ядра. В процессе компиляции и сборки модуля ядра, мы встраиваем уникальный цифровой водяной знак, который содержит информацию о подлинности и идентификации кода. Цифровой водяной знак, внедренный в ядро, становится неотъемлемой частью его структуры. Этот метод позволяет нам не только защитить ядро от несанкционированных изменений, но и значительно улучшить обнаружение поддельных или модифицированных версий кода. В случае любых попыток модификации ядра, цифровой водяной знак будет потерян, что сигнализирует об потенциальной угрозе безопасности системы. Данный метод внедрения цифрового водяного знака в ядро операционной системы Linux предоставляет несколько существенных преимуществ. Во-первых, он обеспечивает дополнительный уровень защиты от несанкционированных изменений, что особенно важно в контексте информационной безопасности. Во-вторых, он помогает в улучшении обнаружения поддельных или модифицированных версий кода ядра, что может существенно повысить надежность системы

В заключении было рассмотрено несколько существующих методов исследования целостности операционной системы Linux и представили наш инновационный метод внедрения цифрового водяного знака. Далее, в следующих главах, мы более подробно опишем разработку и реализацию этого метода, а также представим результаты экспериментов, подтверждающие его эффективность и преимущества в обеспечении целостности Linux-системы в процессе её работы.

СПИСОК ЛИТЕРАТУРЫ

1. Цифровая стеганография и цифровые водяные знаки: в 2 ч. СПб: СПбГУТ, 2016.
2. Цифровые водяные знаки / В. И. Коржик, С. О. Анфиногенов, А. И. Кочкарев [и др.]. 2017. Ч. 2. 197 с.
3. Штеренберг С. И., Красов А. В. Разработка методики построения доверенной среды на основе скрытого программного агента. Ч. 3. Принцип действия программного агента и проверка его работоспособности // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 34-40.
4. Красов А. В., Борисов В. И. Исследование применимости известных методов внедрения цифровых водяных знаков к исполняемым файлам Unix-подобных систем // Известия высших учебных заведений. Технология легкой промышленности. 2022. Т. 56, № 2. С. 38-42.
5. Красов А. В. Метод защиты авторских прав и целостности программного обеспечения на основе внедрения ЦВЗ в исполняемый код // Перспективы науки. 2022. № 4(151). С. 16-25.

УДК 81.322.2

СРАВНИТЕЛЬНЫЙ АНАЛИЗ БИБЛИОТЕК ДЛЯ РЕШЕНИЯ ЗАДАЧ ОБРАБОТКИ ЕСТЕСТВЕННОГО ЯЗЫКА

Копытова Елена Вячеславовна, Филиппов Феликс Васильевич
Санкт–Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч–Бруевича
Большевиков пр., 22/1, Санкт–Петербург, 193232, Россия
e–mails: el.kop16@gmail.com, 9000096@mail.ru

Аннотация. Рассматриваются популярные библиотеки и инструменты для обработки естественного языка. Проводится сравнительный анализ, выявляются преимущества и недостатки каждой библиотеки, тем самым определяя наиболее подходящую для решения конкретных задач.

Ключевые слова: инфокоммуникационные технологии; обработка естественного языка; естественный язык; инструментарий обработки естественного языка; критерии сравнения.

COMPARATIVE ANALYSIS OF LIBRARIES FOR NATURAL LANGUAGE PROCESSING TASKS

Kopytova Elena, Philippov Felix
The Bonch–Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e–mails: el.kop16@gmail.com, 9000096@mail.ru

Abstract. Popular libraries and tools for natural language processing are considered. A comparative analysis is carried out, the advantages and disadvantages of each library are identified, thus determining the most appropriate one for solving specific problems.

Keywords: information and communication technologies; natural language processing; natural language tools; natural language processing tools; comparison criteria.

Обработка естественного языка (Natural Language Processing, NLP) является одной из наиболее активно развивающихся областей искусственного интеллекта. Существует множество библиотек и инструментов, которые помогают разработчикам создавать приложения, использующие технологии NLP [1]. Однако, выбор библиотеки может в значительной степени влиять на качество и эффективность решения задач обработки естественного языка. В данной работе мы представим обзор и сравнительный анализ нескольких популярных библиотек для решения задач обработки естественного языка, таких как: Natural Language Toolkit (NLTK), Stanford CoreNLP, Apache OpenNLP, spaCy и Gensim. Целью данного исследования является выявление преимуществ и недостатков каждой библиотеки, а также определение наиболее подходящей библиотеки для решения конкретных задач обработки естественного языка. Полученные результаты могут быть полезными для разработчиков, исследователей и всех тех, кто занимается обработкой естественного языка.

Natural Language Processing (NLP) — это область искусственного интеллекта, которая занимается обработкой естественного языка. Существует множество библиотек и инструментов, которые помогают разработчикам создавать приложения, использующие технологии NLP.

С помощью сравнительного анализа исследователь может по достоинству оценить все стороны объекта исследования. Делается это путем проведения аналогии между изучаемым «ядром» и аналогичным предметом/явлением, а в дальнейшем автор сравнивает каждый отдельный элемент или объект в целом, выявляя тем самым сходства и отличия, тенденции и отклонения [2].

Решение задач обработки естественного языка актуально во многих предметных областях, включая:

1. Компьютерные науки: обработка естественного языка используется для создания интеллектуальных систем, которые могут понимать и генерировать естественный язык. Это может включать создание чат–ботов, анализ текстов, распознавание речи и машинный перевод.

2. Медицина: обработка естественного языка используется для анализа медицинских записей и документации, а также для создания интеллектуальных систем, которые могут помочь врачам в диагностике и лечении пациентов.

3. Финансы: обработка естественного языка используется для анализа финансовых отчетов, новостей и социальных медиа, чтобы помочь инвесторам и трейдерам принимать решения.

4. Образование: обработка естественного языка используется для создания интеллектуальных систем, которые могут помочь студентам в изучении языков и предметов.

5. Биотехнологии: обработка естественного языка используется для анализа геномных данных и медицинских записей, а также для создания интеллектуальных систем, которые могут помочь в биоинформатике и биомедицинских исследованиях.

Существует множество языков программирования, которые могут использоваться для решения задач обработки естественного языка (Natural Language Processing, NLP). Некоторые из наиболее популярных языков программирования для NLP включают в себя:

1. Python — это один из самых популярных языков программирования для решения задач NLP. В Python существует множество библиотек, таких как NLTK, Spacy, Gensim и другие, которые облегчают работу с задачами обработки естественного языка.

2. Java — это еще один популярный язык программирования для NLP. В Java существует множество библиотек, таких как OpenNLP, Stanford NLP и другие, которые могут помочь в решении задач обработки естественного языка.

3. C++ — это язык программирования, который часто используется для разработки высокопроизводительных систем и библиотек для NLP, таких как Mallet и другие.

4. R — это язык программирования, который часто используется для анализа данных и статистических вычислений. В R существует множество библиотек, таких как tm, quanteda и другие, которые могут помочь в работе с задачами обработки естественного языка.

5. JavaScript — это язык программирования, который используется для разработки веб–приложений. Существуют библиотеки, такие как NaturalNode и другие, которые могут помочь в решении задач обработки естественного языка на JavaScript.

Это лишь несколько примеров языков программирования, которые могут использоваться для решения задач обработки естественного языка. Выбор языка зависит от конкретной задачи и предпочтений программиста.

Разберем пять популярных библиотек на языке программирования Python: Natural Language Toolkit (NLTK), Stanford CoreNLP, Apache OpenNLP, spaCy и Gensim [3].

Natural Language Toolkit (NLTK) — это одна из наиболее популярных библиотек для обработки естественного языка. Она предоставляет широкий спектр инструментов для работы с текстом, включая токенизацию, лемматизацию, стемминг, частеречную разметку, анализ тональности и машинный перевод. NLTK также включает в себя множество корпусов текстов на различных языках, которые могут использоваться для обучения моделей.

Stanford CoreNLP — это библиотека для обработки естественного языка, разработанная в университете Стэнфорда. Она предоставляет инструменты для обработки текстов на нескольких языках, включая токенизацию, лемматизацию, частеречную разметку, извлечение именованных сущностей и анализ отношений между ними. CoreNLP также включает в себя инструменты для обработки текстов на других языках, таких как китайский, японский и немецкий.

Apache OpenNLP — это библиотека для обработки естественного языка, разработанная Apache Software Foundation. Она предоставляет инструменты для обработки текстов на нескольких языках, включая токенизацию, лемматизацию, стемминг, частеречную разметку и извлечение именованных сущностей. OpenNLP также включает в себя инструменты для обучения моделей на основе размеченных корпусов текстов.

spaCy — это библиотека предоставляет инструменты для обработки текста на нескольких языках, включая токенизацию, лемматизацию, частеречную разметку, извлечение именованных сущностей и анализ отношений между ними. spaCy также включает в себя инструменты для обучения моделей на основе размеченных корпусов текстов.

Gensim — это библиотека предоставляет инструменты для моделирования тематической структуры текста, включая построение моделей LDA (Latent Dirichlet Allocation) и LSI (Latent Semantic Indexing). Gensim также включает в себя инструменты для работы с корпусами текстов и поиска схожих документов.

NLTK и spaCy обеспечивают широкий спектр инструментов для работы с текстом, в то время как CoreNLP и OpenNLP предоставляют инструменты для обработки текстов на нескольких языках. Gensim, в свою очередь, предоставляет инструменты для моделирования тематической структуры текста.

В целом, выбор библиотеки для решения задач обработки естественного языка зависит от конкретных потребностей и задач. Библиотеки помогают разработчикам создавать приложения, использующие технологии NLP.

Сравнительный анализ, проведенный в ходе исследования, позволил оценить преимущества и недостатки каждой из рассмотренных библиотек. На основании полученных результатов было определено, что выбор библиотеки может значительно влиять на качество и эффективность решения задач обработки естественного языка.

Результаты исследования представляют значимый интерес для разработчиков, исследователей и всех, кто занимается обработкой естественного языка. Они могут служить полезным руководством для выбора наиболее подходящей библиотеки для решения конкретных задач при создании приложений с использованием технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Founta, A.–M., Djouvas, C., & Tsakalidis, A. (2018). Social media analysis: A survey of techniques, tools and platforms. AI Communications, № 31(3), С. 241–254.
2. Юсков В. С., Баранникова И.В. Сравнительный анализ платформ обработки естественного языка // ГИАБ. 2017. № 3. URL: https://cyberleninka.ru/article/n/sravnitelnyy–analiz–platform–obrabotki–estestvennogo–yazyka (дата обращения: 15.06.2023).
3. Кузьмин А. И. Обзор и сравнение популярных инструментов для обработки естественного языка // Международный журнал информационных технологий и энергоэффективности. 2021. Т. 6. № 4(22). С. 24–33.

УДК 004.056

ВЫБОР МОДУЛЯ ЯДРА ОС LINUX ДЛЯ ВНЕДРЕНИЯ ЦВЗ

Красов Андрей Владимирович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
просп. Большевиков 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: krasov@inbox.ru

Аннотация. В данной статье рассматривается выбор модуля ядра ОС Linux для внедрения цифрового водяного знака. Обсуждаются особенности ядра Linux, а также выделяются критерии выбора модуля, включая

алгоритмы внедрения, ресурсоемкость, совместимость, конфиденциальность и безопасность, а также поддержка модуля. Предоставляются рекомендации для принятия информированного решения при выборе модуля ядра Linux для успешной реализации цифрового водяного знака и защиты цифровых данных.

Ключевые слова: ЦВЗ; ОС Linux; модуль безопасности; вложение; целостность.

CHOOSING A LINUX KERNEL MODULE FOR IMPLEMENTING A DIGITAL WATERMARK

Krasov Andrey
St. Petersburg State University of Telecommunications named after Professor M. A. Bonch-Bruevich
22 / 1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: krasov@inbox.ru

Abstract. This article discusses the choice of a Linux kernel module for implementing a digital watermark. The features of the Linux kernel are discussed, and the module selection criteria are highlighted, including implementation algorithms, resource intensity, compatibility, confidentiality and security, as well as module support. Recommendations are provided for making an informed decision when choosing a Linux kernel module for the successful implementation of a digital watermark and digital data protection.

Keywords: CVZ; Linux OS; security module; attachment; integrity.

Введение. С ростом числа цифровых данных, которые пользователи обменивают и хранят в Интернете, обеспечение их безопасности и целостности становится наиболее важной задачей. Цифровой водяной знак - это один из способов защиты данных от несанкционированного использования и распространения. Ядро операционной системы Linux, благодаря своей гибкости и открытому исходному коду, предоставляет отличную платформу для внедрения цифрового водяного знака. В данной статье рассмотрим ключевые аспекты выбора модуля ядра ОС Linux для реализации данного метода защиты.

Ядро Linux - это основная компонента операционной системы Linux, которая обеспечивает основные функции и управление ресурсами компьютера. Структура ядра Linux может быть представлена следующим образом (Рис.1):

Структура ядра Linux достаточно сложна и состоит из множества компонентов (модулей), которые взаимодействуют друг с другом для обеспечения функционирования операционной системы.

Модули ядра Linux являются загружаемыми компонентами, которые могут быть динамически подключены или отключены от ядра во время работы системы. Они представляют собой независимые программные компоненты, которые расширяют функциональность ядра и предоставляют дополнительные возможности.

Структура ядра Linux достаточно сложна и состоит из множества компонентов (модулей), которые взаимодействуют друг с другом для обеспечения функционирования операционной системы [1]. Линукс позволяет собрать структуру своего ядра из различных модулей, что является приоритетным для многих организаций, так как можно собрать ядро под свою систему безопасности.

Критерии выбора модуля ядра для цифрового водяного знака:

При выборе модуля ядра для реализации цифрового водяного знака в ОС Linux следует учитывать следующие факторы:

– Алгоритмы и методы внедрения: Модуль должен поддерживать современные алгоритмы цифрового водяного знака и обладать механизмами для эффективного внедрения в различные типы файлов, такие как изображения, аудио- и видеофайлы.

– Ресурсоемкость: Модуль должен быть оптимизирован для работы в ядре Linux и не влиять на производительность системы. Ресурсоемкость модуля должна быть минимальной, чтобы обеспечивать плавное и эффективное функционирование ОС.

– Совместимость: Модуль должен быть совместим с версией ядра Linux, установленной на целевой системе. Также важно учитывать совместимость с различными дистрибутивами Linux и обеспечение поддержки обновлений.

Развитие и поддержка: Важно выбрать модуль, который активно разрабатывается и поддерживается сообществом разработчиков. Регулярные обновления и исправление возникающих проблем обеспечат надежность и долговечность системы цифрового водяного знака.

Безопасность является одним из основных аспектов корпоративной политики. Поэтому важно обращать внимание на безопасность ядра Linux. Модуль безопасности Linux обеспечивает механизмы контроля доступа, позволяющие управлять правами доступа пользователей и процессов к файлам и ресурсам системы. Это может быть полезным для установки ограничений на доступ к файлам, содержащим цифровой водяной знак, и обеспечения их конфиденциальности и целостности [2]. Также предоставляет возможности аудита и мониторинга системы. Это позволяет отслеживать и регистрировать действия пользователей и процессов, включая операции с файлами и ресурсами, связанными с цифровым водяным знаком. Такой аудит и мониторинг способствуют выявлению и предотвращению несанкционированного использования или изменения водяного знака. Модуль безопасности Linux соответствует множеству стандартов безопасности, таких как SELinux (Security-Enhanced Linux) и AppArmor. Это обеспечивает совместимость и соответствие с требованиями безопасности и политиками безопасности, принятыми в корпоративной среде.

При использовании метода вложения ЦВЗ, основанного на нахождении дуальности кодировки некоторых инструкций. В случае инструкций с двумя регистровыми операндами порядок следования операндов в ModRM-байте и соответствующее изменение бита направления операции в Opcode-байте не влияют на результат дизассемблирования инструкции, затем ЦВЗ зацикливается.

В ходе работы был проведен анализ машинных команд, используемых в системных файлах ядра ОС Linux, в результате которого были выявлены самые распространенных инструкции x86 архитектуры [3].

В результате исследования представлена статистика используемых инструкций для вложения, в сравнении с общим количеством.

При размере модуля безопасности от 5 до 10 Мб (Среднее значение объема данного модуля) количество экземпляров вложенного ЦВЗ [4] предложенным методом, варьируется от 165 до 330. Этого достаточно для стойкости ЦВЗ, так как при различного рода атаках, может теряться несколько экземпляров вложенной информации, поэтому, чем их больше, тем выше стойкость [5].

В ходе исследования был выбран модуль безопасности ядра ОС Linux для внедрения цифрового водяного знака. При выборе модуля учитывались различные критерии, включая алгоритмы внедрения, ресурсоемкость, совместимость, конфиденциальность, безопасность и поддержка модуля. Результаты исследования были представлены в статье, где приведены рекомендации для принятия информированного решения при выборе модуля ядра Linux для успешной реализации цифрового водяного знака и защиты цифровых данных.

Один из важных выводов исследования заключается в том, что размер модуля безопасности играет существенную роль в возможности вложения большого количества экземпляров цифрового водяного знака, что повышает его стойкость. С увеличением размера модуля безопасности открываются больше возможностей для внедрения и хранения цифрового водяного знака, что делает его более устойчивым к различным атакам и позволяет повысить уровень защиты данных.

СПИСОК ЛИТЕРАТУРЫ

1. Катасонов А. И., Красов А. В., Цветков А. Ю. Разработка универсального алгоритма по созданию простейших модулей ядра для различных версий ядра LINUX // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сборник научных статей: в 4 х т., Санкт-Петербург, 24–25 февраля 2021 г. СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2021. Т. 1. С. 438-442. EDN VOMLVL.
2. Красов А. В. Методика построения доверенной среды в UNIX-подобных ОС на основе внедрения ЦВЗ // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 4. С. 17-25. DOI 10.46418/2079-8199_2020_4_3. EDN IAEQUF.
3. Krasov A. V., Shterenberg S. I Methods for building a trusted environment in UNIX operating systems based on the implementation of a digital watermark // 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT 2020. Brno, 2020. С. 253-257.
4. Шариков П. И., Красов А. В., Штеренберг С. И. Методика создания и вложения цифрового водяного знака в исполняемые JAVA файлы на основе замен опкодов // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 3. С. 66-70. EDN YKVPJF.
5. Красов А. В., Верещагин А. С. Классификация методов скрытого вложения информации в исполняемые файлы // 63-я научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов : материалы. Санкт-Петербург, 21–25 февраля 2011 года. Ч. 1. СПб. : Санкт-Петербургский государственный университет телекоммуникаций имени проф. М. А. Бонч-Бруевича, 2011. С. 216-217. EDN SBASLS.

УДК 004.056

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ В НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЯХ

Литвинов Владислав Леонидович, Балакирев Николай Александрович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
email: vlad.litvinov61@gmail.com, nba11922009@yandex.ru

Аннотация. Современные технологии разработки и эксплуатации нейронных сетей уязвимы для компьютерных атак различного вида. В работе рассмотрены ключевые аспекты информационной безопасности, которые следует учитывать при использовании нейронных сетей, такие как защита данных, включая их шифрование и управление доступом, анонимизация данных и защита нейросетевой модели от несанкционированного доступа, внедрение программных закладок. Важную роль играет мониторинг и обнаружение инцидентов информационной безопасности, а также обучение на защищенных данных. В целом, понимание и применение этих аспектов позволяют снизить риски нарушения конфиденциальности данных и обеспечить безопасность в процессе использования нейронных сетей.

Ключевые слова: информационная безопасность; нейронная сеть; защита данных; конфиденциальность данных.

THREATS TO INFORMATION SECURITY IN NEURAL NETWORK TECHNOLOGIES

Litvinov Vladislav, Balakirev Nikolai
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: vlad.litvinov61@gmail.com, nba11922009@yandex.ru

Abstract. Modern technologies for the development and operation of neural networks are vulnerable to various types of computer attacks. The paper considers key aspects of information security that should be taken into account when using neural networks, such as data protection, including encryption and access control, data anonymization and protection of the neural network model from unauthorized access, the introduction of program bookmarks. An important role is played by monitoring and detection of information security incidents, as well as training on protected data. In general, understanding and applying these aspects can reduce the risks of data privacy violations and ensure security in the process of using neural networks.

Keywords: information security; neural network; data protection; data confidentiality.

Информационная безопасность нейросетевых технологий играет важную роль в защите данных и обеспечении конфиденциальности [1, 2]. Безопасность общедоступных моделей машинного обучения стала критической проблемой. Например, программные закладки могут оставаться скрытыми неопределенное время, пока не будут активированы вводом модифицированных данных, содержащих триггеры. Такие закладки представляют непосредственную угрозу безопасности информации для всех компонентов системы искусственного интеллекта и приводят к ухудшению качества или полному прекращению функционирования систем искусственного интеллекта. Закладки могут быть вставлены в нейронную сеть либо во время обучения, например, сотрудником компании, ответственным за обучение модели, либо при ее адаптации (трансфертное обучение) [3].

Метод защиты нейронных сетей от атак с внедрением закладок включает в себя следующие фазы: выявление закладки; идентификация триггера; нейтрализация закладки. Также существует более новый подход — троянская атака, для проведения которой нет необходимости иметь доступ к обучающему набору данных. Вместо этого подбираются триггеры, которые вызывают максимальный отклик определенных нейронов сети. Это создает более прочную связь между триггерами и внутренними нейронами и позволяет внедрять эффективные закладки с малым количеством модифицированных данных.

Рассмотрим следующий сценарий. Компания публикует свои автономные приложения, которые могут быть загружены и развернуты на беспилотном транспортном средстве. Атакующий загружает нейронную сеть, вводит вредоносное поведение, которое активируется, когда присутствует какой-либо специальный знак на обочине. Затем он публикует их измененными. Они обладают полностью нормальным поведением из-за отсутствия специального знака и различий между двумя моделями. Выявить их неправильное поведение очень трудно. Аналогичные атаки могут быть проведены и на других устройствах. Например, для распознавания лиц может быть введено дополнительное поведение, так что злоумышленник может маскироваться под конкретного человека со специальной меткой. Таким образом, анимация любого постороннего лица с меткой всегда распознается как замаскированная цель. Такие атаки получили название сетевых троянских атак [4].

Даже если модель шифруется при оптимизации, то в процессе исполнения дешифруется, и в рамках OpenSource фреймворка может быть достаточно просто преобразована недобросовестным пользователем в исходную, доступную к копированию и тиражированию. В этом случае возможна сборка системы инференса нейронных сетей (инференс – непрерывная работа какой-либо нейронной сети на конечном устройстве) в рамках одного исполняемого файла с жесткой привязкой к аппаратному ключу, где происходит шифрование части редко используемых функций [5].

В работе подробно рассмотрены ключевые аспекты информационной безопасности, которые следует учитывать при использовании нейронных сетей.

1. Защита данных. Важно обеспечить безопасность данных, используемых для обучения и тестирования нейронной сети. Это включает защиту от несанкционированного доступа, изменения и утечки данных. Рекомендуется использовать шифрование данных в покое и в передаче, а также установить механизмы контроля доступа для ограничения прав доступа к данным.

2. Анонимизация данных. При работе с конфиденциальными данными следует принять меры для анонимизации, чтобы предотвратить идентификацию конкретных лиц или организаций. Это может включать удаление лично идентифицируемых данных или замену их на искусственные значения.

3. Защита модели. Модель нейронной сети является ценным активом и должна быть защищена от несанкционированного доступа и копирования. Рекомендуется использовать механизмы шифрования и цифровой подписи для защиты модели и предотвращения ее изменений или подмены.

4. Уязвимости модели. Нейронные сети могут быть подвержены различным видам атак, включая атаки на входные данные (например, ввод маскировки или внедрение шума) и атаки на модель (например, атаки переноса или отклонения) [6]. Важно проводить анализ уязвимостей модели и принимать меры для ее защиты, такие как использование регуляризации, обнаружение аномалий и мониторинг атак.

5. Мониторинг и обнаружение инцидентов. Необходимо установить механизмы мониторинга и обнаружения потенциальных инцидентов информационной безопасности. Это может включать мониторинг активности пользователей, обнаружение необычных моделей поведения или мониторинг сетевого трафика для выявления атак.

6. Обучение на защищенных данных. Использование защищенных данных для обучения модели может помочь в предотвращении утечек информации или злоумышленного использования. Это может включать

применение техник дифференциальной конфиденциальности или агрегации данных из разных источников без раскрытия конкретных значений.

7. Резервное копирование данных и модели. Регулярное создание резервных копий данных и модели является важным аспектом информационной безопасности. Это помогает предотвратить потерю данных в случае сбоев или катастрофических событий, а также обеспечивает возможность восстановления системы.

8. Обновления и патчи. Регулярное обновление и установка патчей для программного обеспечения, используемого с нейронными сетями, помогает предотвратить уязвимости и обеспечить безопасность системы. Это включает как саму нейронную сеть, так и другие компоненты, такие как фреймворки машинного обучения или операционные системы.

9. Обучение персонала. Обучение и осведомление персонала о принципах информационной безопасности являются важной составляющей безопасного использования нейронных сетей. Персонал должен быть осведомлен о возможных угрозах, процедурах защиты и мероприятиях по обеспечению безопасности данных и моделей.

Например, используя аппаратные ключи, можно обезопасить себя одним из двух способов:

– Использовать API, которое предоставляется производителем, и перенести ключевую логику работы на ключ.

– Воспользоваться программой Virbox Protector. Она анализирует выполняемый файл и предоставляет выбор доступных функций, которые можно защитить разными методами (Obfuscation, Virtualization, Snippet, Encryption). Естественно, использование множества защищённых функций может привести к снижению производительности программы, но при грамотном подходе это будут незначительные потери. Также в Virbox Protector присутствует функция анти-дебаггера, предотвращающая отладку зашифрованной программы, а также дополнительная программа DS Protector, нацеленная на защиту файлов с данными (в нашем случае, модель нейронной сети) с используемой зашифрованной программой [5].

Учитывая эти аспекты информационной безопасности, можно снизить риск нарушения конфиденциальности данных и обеспечить безопасное использование нейронных сетей в интеллектуальных информационных системах.

СПИСОК ЛИТЕРАТУРЫ

1. База угроз безопасности информации ФСТЭК [Электронный ресурс]. URL: https://bdu.fstec.ru/threat (дата обращения 01.02.2022).
2. Xu Q., Arafin M.T., Qu G. Security of neural networks from hardware perspective: A survey and beyond // Proc. of the 26th Asia and South Pacific Design Automation Conference (ASP-DAC). 2021. P. 449-454.
3. Менисов А. Б., Ломако А. Г., Дудкин А. С. Метод защиты нейронных сетей от компьютерных бэкдор-атак на основе идентификации триггеров закладок // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 4. С. 742–750.
4. Liu Y., Ma S., Aafer Y., Lee W.-C., Zhai J. Trojaning attack on neural networks [Электронный ресурс]. URL: https://www.semanticscholar.org/paper/Trojaning-Attack-on-Neural-Networks-Liu-Ma/08f7ac64b420210aa46fcbbdb0f206215f2e0644.
5. Защита моделей нейронных сетей при помощи аппаратных ключей SenseLock [Электронный ресурс]. URL: https://habr.com/ru/articles/555312/ (дата обращения 26.06.2023).
6. Bishop C. M. Pattern Recognition and Machine Learning. Springer, 2006. 738 p.

УДК 004.056.56

ПРИНЦИПЫ БЕЗОПАСНОГО ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Литвинов Владислав Леонидович, Безкоровайная Мария Валерьевна,
Толмачев Андрей Юрьевич, Гольдес Илья Станиславович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: vlad.litvinov61@gmail.com, mashabezk@gmail.com, andreytolmachev03@gmail.com, iliagoldes@gmail.com

Аннотация. В связи с востребованностью в современном обществе информационных систем и технологий появляется все больше рисков, связанных с безопасностью и конфиденциальностью информации. Для того, чтобы минимизировать потенциальные проблемы, необходимо при проектировании учитывать принципы безопасности. В статье рассматриваются основные принципы безопасного проектирования, такие как настройка системы доступа, принцип шифрования данных и их защиты, простота системы, использование безопасных протоколов и другие.

Ключевые слова: информационные системы и технологии; защита данных; безопасное проектирование систем; обеспечение безопасности.

PRINCIPLES OF SAFE DESIGN OF INFORMATION SYSTEMS

Litvinov Vladislav, Bezkorovayinya Maria, Tolmachev Andrey, Goldes Ilya
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: vlad.litvinov61@gmail.com, mashabezk@gmail.com, andreytolmachev03@gmail.com, iliagoldes@gmail.com

Abstract. Due to the demand for information systems and technologies in modern society, there are more and more risks associated with the security and confidentiality of information. In order to minimize potential problems, it is necessary to take into account the principles of safety when designing. The article discusses the basic principles of secure

design, such as setting up an access system, the principle of data encryption and protection, the simplicity of the system, the use of secure protocols, and others.

Keywords: information systems and technologies; data protection; secure system design; security.

Безопасное проектирование информационных систем и технологий — это процесс создания информационных систем и технологий, обеспечивающий безопасность пользователей и их данных [1].

В работе рассмотрены основные принципы безопасного проектирования [2-4].

Настройка системы доступа. Для предотвращения несанкционированного доступа к системе необходимо предоставить только необходимые права доступа. Каждому пользователю выдается доступ к информации в соответствии с полученными полномочиями. Для получения доступа к сервису, работающему с конфиденциальной информацией, использовать различные методы аутентификации, такие как пароли, биометрические данные. Сейчас идет активный переход на использование двухфакторной аутентификации для идентификации пользователя. Шифрование данных обеспечивает конфиденциальность передаваемой и хранимой информации.

Использование безопасных протоколов, которые будут гарантировать конфиденциальность и целостность данных при работе. Простота системы и ее использования помогает избежать непреднамеренных ошибок пользователей в процессе использования и возможного снижения уровня безопасности системы. Простота защиты повышает ее надежность, экономичность, уменьшает ее влияние на вероятностные характеристики системы, создает удобства в обращении с нею.

При проектировании информационных систем и технологий важно учитывать взаимодействие используемых компонентов безопасности между собой. Если компоненты не могут работать вместе, то может возникнуть ряд проблем, таких как блокировка одного компонента другим, снижение производительности, что может привести к уязвимостям в системе. Чтобы избежать таких проблем, применяют специальные интеграционные решения. Обеспечение информацией о используемых защитных средствах только определенного числа лиц.

Таким образом, при проектировании систем и технологий необходимо учитывать множество аспектов для обеспечения безопасности и защиты данных, необходимо контролировать процесс на каждом этапе для выявления возможных каналов утечки информации и получения к ней несанкционированного доступа, а также необходимо, чтобы средства, обеспечивающие безопасность, не ухудшали характеристики системы: производительность и быстродействие.

СПИСОК ЛИТЕРАТУРЫ

1. Проектирование информационной системы. [Электронный ресурс]. URL: https://finswin.com/projects/proektirovanie/informacionnyh-sistem.html. (дата обращения: 25.06.2023).
2. Принципы информационной безопасности. [Электронный ресурс]. URL: https://arinteg.ru/articles/printsipy-informatsionnoy-bezopasnosti-26490.html. (дата обращения: 25.06.2023).
3. Ананьев А. С., Бутенко Д. В., Попов К. В. Интеллектуальные технологии проектирования информационных систем. Методика проектирования программных продуктов в условиях наличия прототипа // Инженерный вестник Дона, 2012. № 2. С. 100-105.
4. Основные принципы проектирования систем обеспечения безопасности информации в автоматизированных системах обработки информации. [Электронный ресурс]. URL: https://studref.com/482364/informatika/osnovnye_printsipy_proektirovaniya_sistem_obespecheniya_bezopasnosti_informatsii_avtomatizirovannyh_siste. (дата обращения: 25.06.2023).

УДК 004.01

ИССЛЕДОВАНИЕ МЕТОДОВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПРОЦЕССОВ РАСПРОСТРАНЕНИЯ ЭПИДЕМИИ

Литвинов Владислав Леонидович, Дергачев Даниил Денисович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков, пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: vlad.litvinov61@gmail.com, ghost1342@gmail.com

Аннотация. Целью исследования является анализ современных подходов к имитационному моделированию процессов распространения эпидемии. В работе рассмотрены компартментные модели распространения инфекционных заболеваний, описание их принципов работы, недостатков и преимуществ перед другими моделями.

Ключевые слова: сложная информационная система; имитационное моделирование; AnyLogic.

RESEARCH OF SIMULATION MODELING METHODS THE PROCESSES OF THE SPREAD OF THE EPIDEMIC

Litvinov Vladislav, Dergachev Daniil
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: vlad.litvinov61@gmail.com, ghost1342@gmail.com

Abstract. The purpose of the study is to analyze modern approaches to simulation modeling of the epidemic spread processes. The paper considers the compartment models of the spread of infectious diseases, the description of their principles of operation, disadvantages and advantages over other models.

Keywords: complex information system; simulation modeling; AnyLogic.

Компартментные модели используются для упрощения математического моделирования процессов распространения инфекционных заболеваний. В этих моделях популяция исследуемого объекта разделяется на различные группы с учетом характера и скорости перемещения между ними. Заболевания, которые дают иммунитет, имеют компартментную структуру, которая отличается от болезней, не связанных с иммунитетом. Для работы с компартментными моделями чаще всего используются обыкновенные дифференциальные уравнения, однако можно использовать и стохастическую (случайную) структуру, которая более реалистична, но гораздо сложнее для анализа.

Существует множество модификаций модели SIR [1] Кермака и Маккендрика (1927), включая те, которые учитывают рождения и смерти, отсутствие иммунитета после выздоровления (модель SIS), короткосрочный иммунитет (SIRS), латентный период заболевания, во время которого человек не является заразным (SEIS и SEIR), и модель MSIR, где младенцы могут быть рождены с иммунитетом. Данные модели позволяют предсказывать распространение болезни, общее число инфицированных, продолжительность эпидемии, а также оценивать различные эпидемиологические параметры. На основе этих моделей можно сделать выводы о том, как различные меры общественного здравоохранения могут повлиять на развитие эпидемии. В работе рассмотрены методы имитационного моделирования на базе этих моделей.

Имитационное моделирование имеет ряд преимуществ перед другими моделями, используемыми в науке и медицине. В первую очередь, этот подход является более точным и позволяет учитывать широкий спектр факторов, влияющих на распространение инфекции. Кроме того, имитационное моделирование является гибким и может быть изменено и дополнено новыми данными, что позволяет делать более точные и предсказуемые прогнозы.

Для реализации работы используется среда AnyLogic [2] — программное обеспечение для имитационного моделирования. Инструмент обладает современным графическим интерфейсом и позволяет использовать язык Java для разработки моделей.

В работе предложена разработанная в среде AnyLogic имитационная модель распространения эпидемии, одной из основных преимуществ которой является агентный подход [3, 4]. С помощью данной методики может быть спрогнозировано число инфицированных, продолжительность эпидемии, вероятность возникновения новых очагов и другие важные эпидемиологические параметры. Также данная модель может показать, как различные меры, такие как карантин, вакцинация, усиление гигиены и т.д., могут повлиять на развитие эпидемии.

СПИСОК ЛИТЕРАТУРЫ

1. The SIR Model for Spread of Disease [Электронный ресурс]. URL: https://services.math.duke.edu/education/ccp/materials/postcalc/sir/sir2.html (дата обращения 25.06.2023).
2. AnyLogic. Системная динамика. [Электронный ресурс]. URL: https://www.anylogic.ru/use-of-simulation (дата обращения 25.06.2023).
3. Taylor A. Introduction to Agent-Based Modeling: Modeling Natural, Social, and Engineered Complex Systems with NetLogo. MIT Press, 2018.
4. Macal Charles M., Michael J. North. Tutorial on agent-based modeling and simulation. // Journal of Simulation, 2010. Vol. 4. № 3. Pp. 151-162.

УДК 004.056

РАЗВИТИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ ВРЕДОНОСНОГО ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Литвинов Владислав Леонидович, Гольдес Илья Станиславович,
Безкоровайная Мария Валерьевна, Толмачев Андрей Юрьевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: vlad.litvinov61@gmail.com, mashabezk@gmail.com, andreytolmachev03@gmail.com, iliagoldes@gmail.com

Аннотация. В статье рассматриваются актуальные угрозы, возникающие с развитием искусственного интеллекта вследствие его злонамеренного применения. Проанализированы примеры подобного использования искусственного интеллекта, определены цели и задачи таких действий, а также способы регулирования. Рассмотрена необходимость анализа и реакции со стороны общества и государственных органов власти на данную проблему.

Ключевые слова: искусственный интеллект; злонамеренное использование искусственного интеллекта; информационная безопасность; информационно-психологическая безопасность.

DEVELOPMENT OF MEANS TO PROTECT INFORMATION SYSTEMS FROM THE MALICIOUS USE OF ARTIFICIAL INTELLIGENCE

Litvinov Vladislav, Goldes Ilya, Bezkorovayinya Maria, Tolmachev Andrey
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: vlad.litvinov61@gmail.com, mashabezk@gmail.com, andreytolmachev03@gmail.com, iliagoldes@gmail.com

Abstract. The article discusses the current threats that arise with the development of artificial intelligence due to its malicious use. Examples of such use of artificial intelligence were analyzed, the goals and objectives of such actions, as well as methods of regulation were determined. The necessity of analysis and reaction on the part of society and state authorities to this problem is considered.

Keywords: artificial intelligence; malicious use of artificial intelligence; information security; psychological security.

В последнее время прогресс в развитии систем искусственного интеллекта (ИИ) позволил выйти на новый уровень оценки как перспектив развития человеческой цивилизации на основе подобных технологий, так и угроз, связанных с их применением. При этом, имеет место не только опасность ИИ самого по себе, но и опасность от злонамеренного использования искусственного интеллекта определенными лицами (ЗИИИ).

Одной из проблем, сопровождающей развитие ИИ, является быстрый внедрения ИИ в общественную жизнь и его возможностей, за которым не поспевают как правовое регулирование в отдельных странах и существующие механизмы контроля, так и система международного права. Большая часть опасений связана с угрозами, исходящими не от ИИ как такового, а от ЗИИИ, как антисоциальное применение ИИ в интересах государственных и негосударственных акторов [1].

Одним из существующих примеров ЗИИИ является злонамеренное использование технологии «глубоких фейков» (deepfakes) — метода синтеза человеческого изображения и/или голоса на основе использования ИИ. В настоящий момент известны случаи использования глубоких фейков для вымогательства и шантажа, клеветы, возбуждения ненависти и т.п. ЗИИИ может также представлять собой неоправданное использование дронов, угрозы кибератак на элементы инфраструктуры, манипуляции с криптовалютами, использование ботов в компаниях по подрыву репутации отдельных личностей, организаций, стран и многое другое.

Для предотвращения ЗИИИ, помимо мер информационной безопасности может потребоваться создание дисциплинарных групп специалистов по исследованию информационно-психологических аспектов ЗИИИ. Подобные группы могли бы, используя методы сценарного анализа и ряд других, создавать схемы не только технической диагностики deepfakes и других технологий, но и методы информационно-психологического противодействия с использованием ИИ [2, 3].

Таким образом, необходимо всестороннее развитие индивидов, которые, имея навыки критического мышления, смогут практически всегда защищаться от ЗИИИ. Также важно, чтобы с развитием ИИ правовое регулирование отдельных стран было способно регулировать злонамеренное использование ИИ. На данный момент, очевидно, что при злонамеренном использовании слабого ИИ, выступающего в роли инструмента для ограниченного числа задач, виновным является лицо, являющееся исполнителем. Однако при создании гипотетического сильного ИИ встает вопрос, является ли он субъектом преступления или способом его совершения.

СПИСОК ЛИТЕРАТУРЫ

1. Пашенцев Е. Н. Злонамеренное использование искусственного интеллекта: новые угрозы для международной информационно психологической безопасности и пути их нейтрализации. // Государственное управление. Электронный вестник. 2019. № 76. С. 279-300.
2. Угрозы злонамеренного использования искусственного интеллекта против России и Вьетнама в Северо-Восточной Азии / Д. Ю. Базаркина [и др.] // Социально-гуманитарные знания. 2021. № 4. С. 212-234.
3. Аверинская С. А., Севостьянова А. А. Создание искусственного интеллекта с целью злонамеренного использования в уголовном праве Российской Федерации // Закон и право. 2019. № 2. С. 94-96.

УДК 004.056

АНАЛИЗ АТАК НА СЕТЕВЫЕ УЗЛЫ ГРУППОВЫХ РОБОТОВ

Литвинов Владислав Леонидович, Яшин Алексей Владимирович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: vlad.litvinov61@gmail.com, alexey.morris@gmail.com

Аннотация. В работе рассмотрены угрозы на сетевые узлы групповых роботов для нарушения алгоритмов их функционирования и предложены методы защиты от атак нарушителя с использованием нескольких параметров для оценки доверия.

Ключевые слова: сетевые узлы; кибертаки; групповые роботы; защита информации.

ANALYSIS OF ATTACKS ON THE NETWORK NODES OF GROUP ROBOTS

Litvinov Vladislav, Yashin Alexey
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: vlad.litvinov61@gmail.com, alexey.morris@gmail.com

Abstract. The paper considers threats to the network nodes of group robots to disrupt their functioning algorithms and suggests methods of protection against intruder attacks using several parameters to assess trust.

Keywords: network nodes; cyberattacks; group work; data protection.

В настоящее время робототехника активно развивается и внедряется в различные сферы жизни человека. Применение групп роботов повышает их эффективность и возможности, позволяя выполнять задачи разной степени сложности. Для дистанционного управления роботами используется огромное количество сетевых протоколов и инструментов для создания программного обеспечения. Бортовые контроллеры могут поддерживать такие технологии как Blueetooth, инфракрасный порт, ZigBee [1].

При использовании сетевых протоколов, встает вопрос о безопасной передаче данных между узлом управления и роботами. При выполнении задачи роботы или сенсорные узлы обмениваются между собой информацией, причем данный процесс структурирован согласно четкому алгоритму. Лидер группы задает темп, разделяя время работы на активные и неактивные фазы. Каждая активная фаза начинается с посылки специального пакета-маячка, который подчиненные узлы используют для синхронизации своей активности. Злоумышленники могут воздействовать на процессы передачи данных, что приведет к загруженности узлов сети и различным ошибкам [2]. Рассмотрим основные виды угроз.

Угроза перехвата процессом кластеризации систем группового управления роботами.

– Эта угроза заключается в том, что нарушитель получает несанкционированный доступ к узлам управления, что приводит к доступу в систему и перехвату информации по беспроводному каналу связи. Данная угроза возможна при условии генерации поддельных пакетов, которые содержат искаженные данные, а также более мощного приемника.

– Угроза подмены данных об узле путем посылки ложный сообщений.

– Данный вид угрозы заключается в том, что в некоторых системах группового управления узлы отправляют не только свои данные, но и данные соседних узлов. Нарушитель может отправлять ложные данные об узле, перехватывать подлинный узел связи и внедрять собственный узел связи для выполнения задачи и в дальнейшем нарушения процессов работы.

– Угроза искажения информации о целях, передаваемых для составления общей матрицы целей.

– Узлы группы передают информацию о выполнении цели из списка целей. Нарушитель посылает данные об успешном выполнении цели, тем самым цель не выполняется, что приводит к нарушению работы в системе.

– Многие угрозы описанные выше связаны с воздействием на лидера группы и базовые процессы. Для защиты информации в работе предлагается использовать защищенные алгоритмы с вычислением значения доверия (взаимная аутентификация абонентов при установлении соединения).

Данный подход основам на использовании нескольких параметров для оценки доверия, что позволяет противодействовать множеству различных кибератак. Такими параметрами могут быть, например, количество принятых, отправленных, отброшенных пакетов, загруженность узла [3].

СПИСОК ЛИТЕРАТУРЫ

1. Дееф Ф. Дистанционное управление мобильным роботом на основе протокола Zigbee // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова, Белгород, 01–30 мая 2015 года. Б.: БГТУ им. В.Г. Шухова, 2015. С. 2822-2825.
2. Басан Е. С., Басан А. С., Макаревич О. Б., Бабенко Л. К. Исследование влияния активных сетевых атак на группу мобильных роботов [Электронный ресурс] // Вопросы кибербезопасности. 2019. № 1 (29). URL: https://cyberleninka.ru/article/n/issledovanie-vliyaniya-aktivnyh-setevyh-atak-na-gruppu-mobilnyh-robotov (дата обращения: 15.06.2023).
3. Басан А. С., Басан Е. С., Макаревич О. Б. Анализ и разработка средств обеспечения безопасности для систем группового управления автономными мобильными роботами [Электронный ресурс] // Вопросы кибербезопасности. 2017. № 5(24). URL: https://cyberleninka.ru/article/n/analiz-i-razrabotka-sredstv-obespecheniya-bezopasnosti-dlya-sistem-gruppovogo-upravleniya-avtonomnymi-mobilnymi-robotami (дата обращения: 15.06.2023).

УДК 007.3

МЕТОД ФОРМИРОВАНИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ С УЧЕТОМ ИМЕЮЩИХСЯ РЕСУРСОВ

Липатников Валерий Алексеевич, Парфиров Виталий Александрович, Петренко Михаил Игоревич
Военная академия связи им. Маршала Советского Союза С. М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: lipatnikovanl@mail.ru, vitaly.parfirov@yandex.ru, mishany11@mail.ru

Аннотация. На основе методов теорий управления, множеств и комбинаторики разработан метод поиска вариантов управленческих решений (стратегий) по изменению состояния элементов телекоммуникационных сетей специального назначения в целях выполнения заданных требований вышестоящей системы с учетом доступных ресурсов, а также поиска из найденного множества вариантов стратегий оптимальной по заданному критерию. Новизной разработанного метода является то, что в нем учитывается наличие доступных ресурсов по реализации каждого отдельного действия из конкретной стратегии по переводу элементов телекоммуникационной сети в требуемое состояние. Реализация разработанного метода в системах управления телекоммуникационными сетями специального назначения повысит эффективность процесса управлениями качество функционирования телекоммуникационной сети в условиях информационного противоборства.

Ключевые слова: метод управления; ресурс; стратегия управления; оптимизация управления; действия по управлению; телекоммуникационная сеть специального назначения; эффективность управления.

METHOD OF FORMATION OF MANAGEMENT DECISIONSIN SPECIAL PURPOSE TELECOMMUNICATION NETWORKSTAKING INTO ACCOUNT THE AVAILABLE RESOURCES

Lipatnikov Valery, Parfirov Vitaly, Petrenko Mikhail
Marshal of the Soviet Union S.M. Budyonny Military Academy of Communications
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: lipatnikovanl@mail.ru, vitaly.parfirov@yandex.ru, mishany11@mail.ru

Abstract. Based on the methods of management theories, sets and combinatorics, a method has been developed to search for management solutions (strategies) to change the state of elements of special-purpose telecommunication networks in order to meet the specified requirements of a higher-level system, taking into account available resources, as well as to search from the found set of strategy options optimal by a given criterion. The novelty of the developed method is that it takes into account the availability of available resources for the implementation of each individual action from a specific strategy for the transfer of elements of the telecommunications network to the required state. The implementation of the developed method in special-purpose telecommunication network management systems will increase the efficiency of the management process and the quality of the functioning of the telecommunications network in the conditions of information warfare.

Keywords: management method; resource, management strategy; management optimization; management actions; special purpose telecommunication network; management efficiency.

При управлении сложными системами, особенно в процессе их функционирования в условиях информационного конфликта, постоянно требуется решать задачи направленные на определение стратегии приведения системы в требующееся состояние. При этом, практически всегда действовать приходится в условиях ограниченных ресурсов (материальных, временных, людских и т.д.). Так как каждое действие характеризуется определенными затратами, то задача управления состоит в определении оптимальной стратегии поведения с точки зрения минимизации затрат ресурсов [1].

При управлении телекоммуникационными сетями связи специального назначения постоянно приходится решать подобные задачи, так как специфика их функционирования накладывает дополнительные требования нехарактерные для сетей связи общего пользования [2]. На одно из главных мест в данном случае выходят временные параметры реализации того или иного способа повышения (обеспечения) заданного параметра.

Допустим имеется телекоммуникационная сеть специального назначения, содержащая заданное число элементов (узлов коммутации и оконечных устройств). Каждому элементу сети связи доступен перечень действий. При этом, каждое из них характеризуется стоимостью, временем реализации, признаком доступности.

Реализация конкретного действия в возможном наборе действий (стратегии)для любого элемента характеризуется признаком реализации данного действия.

Любая возможная стратегия по приведению телекоммуникационной сети к требуемым показателям качества для достижения целей функционирования, состоящая из определенного количества действий в заданном элементе, характеризуется вектором реализуемых действий.

Таким образом, для каждой стратегии приведения телекоммуникационной сети к удовлетворению целей функционирования для любого элемента сети, характеризуемого вектором действий, можно вычислить временные и стоимостные затраты на ее реализацию. Для этого для элементов вектора:

– определяются значения временных затрат для последовательного и параллельного методов реализации действий над элементами телекоммуникационной сети;

– определяются материальные затраты как сумма произведений признака реализации действия на стоимость реализации данного действия.

Определение оптимальной стратегии по достижению целей функционирования телекоммуникационной сетью для заданного элемента сети выстраивают вариационные ряды по временным и материальным затратам для всех найденных стратегий. По вариационным рядам определяют оптимальную, по заданному критерию, который определяется конкретными условиями функционирования телекоммуникационной сети.

Для определения оптимальной стратегии управления телекоммуникационной сетью требуется проанализировать все доступные варианты стратегий управления каждого элемента телекоммуникационной сети. Вариант реализации разработанного метода формирования управленческих решений (или допустимых стратегий управления) элементами телекоммуникационной сети представлен алгоритмом.

Ключевыми элементами данного алгоритма являются блоки по моделированию применения набора действий и блоки, в которых осуществляется оценка эффективности применения каждого сформированного набора действий. В частности, реализация блоков моделирования и оценки эффективности управления в интересах задач, направленных на снижение доступности элементов сети радиосвязи средствам радионаблюдения злоумышленника, могут быть использованы работы [3-12].

Разработанный метод формирования управленческих решений в телекоммуникационных сетях специального назначения с учетом имеющихся ресурсов позволяет автоматизировать поиск оптимального набора действий в системах поддержки принятия решений в системах управления специальной связью.

СПИСОК ЛИТЕРАТУРЫ

1. Боговик А. В., Игнатов В. В. Теория управления в системах военного назначения : учеб. СПб.: ВАС, 2008. 460 с.
2. Ермишян А. Г. Теоретические основы построения систем военной связи в объединениях и соединениях: Ч. 1. Методологические основы построение организационно-технических систем военной связи. СПб.: ВАС, 2005. 740 с.

3. Парфиров В. А. Математическая модель динамики перемещений локально распределенного группового объекта // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2022. № 9-10 (171-172). С. 50-57.
4. Липатников В. А., Сахаров Д. В., Парфиров В. А., Петренко М. И. Моделирование функционирования распределенного объекта радиоконтроля // Региональная информатикаи информационная безопасность. Юбилейная XVIII Санкт-Петербургская междунар. конф. Санкт-Петербург, 26 — 28 октября 2022 г. : сборник трудов. СПб.: СПОИСУ, 2022. Вып. 11. С. 599-604.
5. Липатников В. А., Сахаров Д. В., Парфиров В. А., Петренко М. И. Имитационная модель распределенного объекта радиоконтроля, отражающая динамику перемещений и смену режимов работы радиоэлектронных средств // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская междунар. конф. Санкт-Петербург, 26 — 28 октября 2022 г. СПб.: СПОИСУ, 2022. С. 556-558.
6. Липатников В. А., Парфиров В. А. Способ моделирования местонахождения объектов группы с учетом динамики перемещений // Инновационная деятельность в Вооруженных Силах Российской Федерации. Труды всеарм. научн.-практич. конф. Санкт-Петербург, 13–14 октября 2022 г. СПб. : ВАС. 2022. С. 253-258.
7. Липатников В. А., Парфиров В. А., Петренко М. И. Общая модель самоорганизующейся сети радиосвязи с мультиплексированием потоков // Транспорт России: проблемы и перспективы. Материалы междунар. научн.-практ. конф. Санкт-Петербург, 9-10 ноября 2022 г. СПб. : Институт проблем транспорта им. Н. С. Соломенко РАН, 2022. Т. 1. С. 293-297.
8. Липатников В. А., Парфиров В. А. Модель процесса наблюдения за множеством источников информации в стохастических условиях // Информация и космос. 2022. № 1. С. 35-44.
9. Липатников В. А., Парфиров В. А. Вероятностно-временные характеристики процесса измерения координат робототехнических комплексов военного назначения по излучаемым радиосигналам // Перспективные системы и задачи управления. XVII Всерос. конф. Карачаево-Черкесская Республика, п. Домбай, 4-8 апр. 2022 г.: сб. трудов. Таганрог : ИП Марук М. Р. 2022. С. 214-220.
10. Липатников В. А., Парфиров В. А. Вероятностные характеристики процесса определения местоположения объектов радиоконтроля с учетом стохастичности параметров излучений и помех // Актуальные проблемы защиты и безопасности. Труды XXV Всерос. научно-практ. конф. Санкт-Петербург, 4-7 апр. 2022 г. Т. 1. СПб. : РАРАН, 2022. С. 299-304.
11. Липатников В. А., Парфиров В. А. Вероятностно-временные показатели процесса выявления сетей радиосвязи // Инновационные технологии и технические средства специального назначения. Труды XV научно-практической конференции : в 2-х т. Санкт-Петербург, 21–22 ноября 2022 г. СПб: БГТУ «Военмех», 2023. С. 172-175.
12. Гладких Д. С., Парфиров В. А., Васильев Н. А. Математическая модель процесса обработки источников радиоизлучений комплексом радиоконтрол // Инновационные достижения и результаты научной деятельности операторов научных рот Вооруженных Сил Российской Федерации : сб. научн. статей по матер. круглого стола. Санкт-Петербург, 29 нояб. 2022 г. Военная академия связи. СПб.: ВАС, 2022. С. 50-57.

УДК 004.056.53

ОБЗОР ИССЛЕДОВАНИЙ ПО ОЦЕНКЕ ПРОИЗВОДИТЕЛЬНОСТИ WLAN СЕТИ

Махмутова Нурия Фаритовна, Ковцур Максим Михайлович,
Петрова Татьяна Васильевна, Кируга Антон Юрьевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: iromup9898@gmail.com, maxkovzur@mail.ru, tanya26012001@mail.ru, anton.kistruga@gmail.com

Аннотация. Рассматриваются различные методики повышения производительности беспроводных сетей с использованием различных критериев, таких как производительность, масштабируемость, энергопотребление и безопасность. В основной части представлены результаты исследований, включающие оценку пропускной способности и задержки передачи данных, измерение задержки передачи данных, исследование масштабируемости, энергопотребления, маршрутизации и передачи данных, а также безопасности беспроводных сетей. Для выбора наилучшего подхода к повышению производительности беспроводной сети рекомендуется учитывать все эти аспекты и использовать критерии, такие как производительность, масштабируемость, энергопотребление и безопасность. Результаты исследований позволяют определить наилучшие методы и рекомендации для разработки более эффективных и безопасных беспроводных сетей.

Ключевые слова: беспроводные сети; производительность; оптимизация; Wi-Fi; технологии оптимизации.

RESEARCH OF METHODS FOR EVALUATING AND IMPROVING THE PERFORMANCE OF A WIRELESS NETWORK

Makhmutova Nuriia, Kovzur Maxim, Petrova Tatiana, Kistruga Anton
Saint Petersburg State University of Telecommunications named after V. I. prof. M. A. Bonch-Bruevich
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: iromup9898@gmail.com, maxkovzur@mail.ru, tanya26012001@mail.ru ,anton.kistruga@gmail.com

Abstract. Various methods of improving the performance of wireless networks using various criteria such as performance, scalability, power consumption and security are considered. The main part presents the results of research, including the assessment of data transmission bandwidth and latency, measurement of data transmission latency, research on scalability, power consumption, routing and data transmission, as well as the security of wireless networks. To choose the best approach to improving wireless network performance, it is recommended to take into account all these aspects and use criteria such as performance, scalability, power consumption and security. The results of the research allow us to determine the best methods and recommendations for the development of more efficient and secure wireless networks.

Keywords: wireless networks; performance; optimization; Wi-Fi; technology optimization.

С ростом количества устройств и объемов, передаваемых данных, возникает необходимость в повышении производительности беспроводных сетей. Быстрый и надежный доступ к данным, высокая пропускная способность и минимальная задержка передачи становятся основными требованиями в условиях современных

деловых и технологических процессов [8-12]. Повышение производительности сети позволяет оптимизировать рабочие процессы, улучшить качество обслуживания, повысить эффективность использования ресурсов и обеспечить более быструю и удобную коммуникацию между устройствами и пользователями. Для этого существуют разные подходы, которые позволяют оценить работу WLAN сетей и улучшить качество обслуживания пользователей. Рассмотрены различные методы повышения производительности беспроводных сетей. Приведены сравнительные критерии, учитывающими производительность, масштабируемость, энергопотребление и безопасность для сравнения эффективности методов [1-7]. Исследования показали, что каждый подход имеет свои плюсы и минусы, и выбор оптимального подхода должен базироваться на конкретных требованиях, ограничениях и условиях применения. Таким образом, различные подходы могут привести к различной оценке производительности беспроводных WLAN сетей. Результаты исследования могут быть использованы для выбора оптимального метода повышения производительности беспроводных сетей и оптимизации качества обслуживания пользователей.

СПИСОК ЛИТЕРАТУРЫ

1. Assessing the Throughput of Wi-Fi Networks Depending on the Frequency Range / Smith J. [et al] // Wireless Communications and Mobile Computing, 2020. [Электронный ресурс] URL: https: Archive : International Journal of Wireless Communications and Mobile Computing (ijwcmc.org) (дата обращения 23.06.2023).
2. Measurement and Analysis of Data Transmission Delay in LTE Wireless Networks / Johnson R. [et al] // IEEE Communications Magazine, 2018. [Электронный ресурс] URL: https: IEEE Xplore (дата обращения 21.06.2023).
3. Scalability in Wireless Networks: Methods and Solutions / Brown A. [et al] // IEEE Communications Surveys & Tutorials, 2019. [Электронный ресурс] URL: https: IEEE Xplore: IEEE Communications Surveys & Tutorials (дата обращения 21.06.2023).
4. Energy Consumption Analysis of Wireless Devices in Different Operating Modes / Anderson L. [et al] // ACM Transactions on Embedded Computing Systems, 2017. [Электронный ресурс] URL: https: On Space Utilization Enhancement of File Systems for Embedded Storage Systems // ACM Transactions on Embedded Computing Systems (дата обращения 23.06.2023).
5. Efficiency Analysis of Routing Protocols in Wireless Networks / Wilson M. [et al] // Wireless Networks, 2020. [Электронный ресурс] URL: https: Wireless Networks | Home (springer.com) (дата обращения 21.06.2023).
6. Quality of Service (QoS) Analysis in Wireless Networks / Davis K. [et al] // IEEE Transactions on Wireless Communications, 2020. [Электронный ресурс] URL: https: IEEE Xplore: IEEE Transactions on Wireless Communications (дата обращения 23.06.2023).
7. Security Analysis of Wireless Networks / Johnson R. [et al] // IEEE Transactions on Dependable and Secure Computing, 2020. [Электронный ресурс] URL: https: IEEE Xplore: IEEE Transactions on Dependable and Secure Computing (дата обращения 23.06.2023).
8. Виткова Л. А., Ахрамеева К. А., Грузинский Б. А. Использование геометрических хеш-функций в информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности. 2017. Т. 37. № 3. С. 5-9.
9. Герлинг Е. Ю., Ахрамеева К. А., Карельский П. В. Исследование влияния естественного шума… изображений, используемых как покрывающие объекты, на эффективность стеганографических атак // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 2. С. 19-23.
10. Калинин М. О., Штеренберг С. И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения // Интеллектуальные технологии на транспорте. 2018. № 3 (15). С. 47 54.
11. Сахаров Д. В., Красов А. В., Ушаков И. А., Бирих Э. В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе ipv6 // Защита информации. Инсайд. 2020. № 1 (91). С. 51-57.
12. Чмутов М. В., Ковцур М. М., Ушаков И. А., Пестов И. Е. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре // Информационная безопасность регионов России (ИБРР-2017) : материалы конференции. 2017. С. 535-537.

УДК 621.391.28

ИССЛЕДОВАНИЕ ПРОГРАММНОЙ СТРУКТУРЫ АРХИТЕКТУРЫ СЕТИ РАДИОДОСТУПА LTE

Мошак Николай Николаевич, Кравец Алексей Юрьевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, Санкт-Петербург, 193323, Россия
e-mails: nnmoshak49@ mail.ru, alexeipyp@gmail.com

Аннотация. Рассматривается программная структура сети радиодоступа LTE. Исследуются особенности протокольной организации уровневых логических соединений архитектуры сети радиодоступа LTE с учетом типа передаваемого трафика. Приводятся форматы и структура уровневых протокольных блоков.

Ключевые слова: LTE; программная структура сети радиодоступа LTE; уровневые протоколы PDCP; RLC; MAC; Ph.

STUDY OF SOFTWARE STRUCTURE OF LTE RADIO ACCESS NETWORK ARCHITECTURE

Moshak Nikolay, Kravets Alexey
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bryuevich
22 Bolshevik’s Av, St. Petersburg, 193323, Russia
e-mails: nnmoshak49 @ mail.ru, alexeipyp@gmail.com

Abstract. The software structure of the LTE radio access network is considered. Features of protocol organization of layer logical connections of LTE radio access network architecture are investigated taking into account type of transmitted traffic. Formats and structure of layer protocol blocks are given.

Keywords: LTE; software structure of the LTE radio access network; layer protocols PDCP; RLC; MAC; Ph.

В логической структуре плоскости пользователя архитектуры сети LTE подмножество функций на участке радиодоступа IP/E-UTRAN (Evolved Universal Terrestrial Radio Access Network) расширено и отличается по своему составу и полноте от классической семиуровневой модели архитектуры BOC [1]. Это связано со спецификой функционирования сети радиодоступа E-UTRAN [2]. Логическая структура архитектуры сети радиодоступа E-UTRAN LTE включает следующие логические уровни:

1) PDCP (Packet Data Convergence Protocol). Подуровень конвергенции пакетов данных обрабатывает данные более высоких уровней: SDU (Service Data Units) — дейтаграммы трафика и сигнальные сообщения. При этом осуществляют: сжатие (и, соответственно, восстановление) IP-заголовков, используя протокол ROHC (Robust Header Compression), шифрацию и дешифрацию SDU трафика и сигнализации, защиту (проверку) целостности сигнальных сообщений. Кроме указанных функций, уровень PDCP обеспечивает передачу данных без потерь при хэндоверах и обрывах связи.

2) RLC (Radio Link Control Protocol). Подуровень управления радиосоединением RLC обеспечивает: сегментацию SDU на PDU (Protocol Data Unit) для передачи и объединение пакетов при приеме в требуемой последовательности, коррекцию ошибок при передаче, используя повторную передачу (ARQ), устранение ошибок в передаче пакетов, вызванных ошибками сигнализации. Возможны три режима обработки пакетов на уровне RLC в зависимости от типа передаваемой информации:

– прозрачный TM (transparent mode) — пакеты не обрабатывают на уровне RLC;
– передача без подтверждения UM (unacknowledged mode);
– передача с подтверждением AM (acknowledged mode).

3) MAC (Medium Access Control Protocol). Подуровень управления доступом к среде MAC осуществляет размещение и мультиплексирование протокольных блоков логических каналов в транспортные с последующей передачей их по физическим каналам. На уровень MAC возложены следующие функции: управление выделением канального ресурса с учетом приоритетов трафика, т.е. выполняют задачи планирования передач (обрабатывает расстановку приоритетов логических каналов для одного и того же UE и динамическое планирование между UE), выбор транспортных форматов передач, управление повторными передачами непринятых пакетов, организацию процедур доступа UE к сети и периодической синхронизации UE, измерения: объема передаваемого трафика, загрузки канала, состояния буферов передачи UE, относительной мощности передачи UE и ряд других, организацию режима сна/прерывистого приема (DRX) абонентских станций, управляет исправлением ошибок HARQ.

4) PHY Физический подуровень обеспечивает перенос информации из транспортных каналов MAC по радиоинтерфейсу. Обеспечивает адаптацию линии, управление мощностью, поиск соты (для целей начальной синхронизации и передачи обслуживания) и другие измерения (внутри системы LTE и между системами) для уровня RRC.

Здесь канальный уровень модели BOC представлен тремя подуровнями: подуровнем сходимости пакетных данных PDCP, подуровнем управления соединением в радиоканале RLC и подуровнем управления доступом к среде MAC.

Программная, структура сети радиодоступа E-UTRAN LTE базируется на декомпозиции иерархии ее программного обеспечения и описывает взаимодействие связанных между собой отдельных программ, отображающих работу и взаимосвязь ее логических уровней. Программная структура сети радиодоступа E-UTRAN LTE в режиме установленной сессии обеспечивает две ключевые сетевые задачи в радиоканале (radio bearer): 1) поддержание изохронности передачи элементов сервисных потоков SDF (Service Data Unit) в выделенных радиоканалах с гарантированной скоростью передачи GBR (Guaranteed Bit Rate) и 2) обеспечение надежной и достоверной передачи элементов потоков SDF в выделенных радиоканалах non-GBR. Для реализации уровневых функций в программной структуре сети радиодоступа E-UTRAN используются различные механизмы их программной реализации, которые осуществляют параметризацию или «окраску» потоков с целью задействования определенных алгоритмов их обслуживания на узлах сети.

Рассмотрим кратко режим сессии [1]. После классификации IP пакеты потока SDF направляются на подуровень сходимости пакетных данных PDCP или подуровень конвергенции пакета радиоканала [3]. Подуровень PDCP предоставляет сервис уровню IP оборудования пользователя в виде логических радиоканалов, адаптируя IP-пакет к пакету радиоканала. Для IP пакетов каждого входного потока на подуровне PDCP определен свой буфер памяти. Протокольный блок уровня PDCP PDU формируется добавлением к IP пакету соответствующего заголовка управляющую информацию PCI (Packet Control Information). Здесь протокольных блоков всего два типа: C/D — «управление»/ «данные». Протокольный блок данных PDCP PDU (Protocol Data Unit) используются для передачи одного IP пакета. При этом каждый протокольный блок PDCP PDU в заголовке «окрашивается» типом входящего потока SDF. Речевой пакет «окрашивается» 7-битным значением номера поля заголовка PDCP «SN», обеспечивая тем самым, сжатие заголовков речевых пакетов (header compression) и их восстановление на уровне PDCP. Пакеты данных «окрашиваются» 12-битный номером PDCP «SN». Заголовки пакетов данных не сжимаются.

После формирования PDCP PDU они поступают на нижележащий подуровень RLC (логический) в соответствующий буфер памяти. Каждый буфер RLC обслуживается определенным протоколом или режимом обслуживания. Подуровень RLC обеспечивает три режима (протокола) обслуживания [4]: режим «прозрачного» обслуживания TM (Transparent Mode Data) для передачи GBR потоков; режим с подтверждением правильного

приема данных AM (Acknowledged Mode Data) для передачи данных non-GBR выделенного канала и режим без подтверждения правильного приема данных UM (Unacknowledged Mode Data) для передачи данных non-GBR невыделенного канала. В режиме с подтверждением подуровень RLC производит сегментацию, объединение и коррекцию ошибок с помощью ARQ, т. е. повторно передает ошибочно принятый блок (при запросе HARQ на MAC уровне). Каждый протокол (TM, UM, AM) формирует соответствующий RLC PDU и также «окрашивает» его в заголовке PCI типом соединения, установленного пользователем.

Протокольные блоки данных RLC SDU TM, RLC SDU UM и RLC SDU AM по логическим каналам, установленным подуровнем MAC (транспортным), поступают на обслуживание или планирование в соответствующий буфер памяти подуровня MAC [5]. Логические каналы — предоставляют услуги подуровня MAC в пределах структуры протокола LTE. Каждый буфер памяти обслуживается планировщиком MAC в интервале планирования TTI (Transmission Time Interval) с частотой 1мс. В процессе обслуживания (планирования) очередей планировщик MAC уведомляет подуровень RLC: когда (в каком TTI), откуда (из какой очереди UE — логического канала TM, UM или AM) и сколько (RLC PDU) из этих очередей на каждом интервале TTI можно передать. В результате обслуживания определенной очереди формируется протокольный блок подуровня MAC PDU (TM, UM, AM) — транспортный блок TB (Transport Block) переменной длины. Каждый заголовок транспортного блока MAC TB «окрашивается» связанным подзаголовком [5]. Подзаголовок содержит идентификатор логического канала (LCID), из которого передан RLC PDU (TM, UM или AM) каждого UE, и длину PDU в байтах. Существует также флаг, указывающий, является ли подзаголовок последним или нет. Один или несколько блоков RLC PDU вместе с заголовком MAC (при необходимости с заполнением для соответствия запланированному размеру транспортного блока) и образуют один TB MAC (TM, UM, AM). Для речевых TB MAC TM организуется «транспарентный» или «прозрачный» режим передачи без образования очередей на транспортном подуровне MAC, что обеспечивает изохронность их передачи. Для TB MAC AM формируются проверочные коды CRC, которые позволяют обнаружить искаженные транспортные блоки на приеме и переспросить их у подуровня RLC, что обеспечивает достоверную и надежную передачу данных. При этом, если размер TB MAC меньше, чем размер одного PDCP PDU данных из которого он состоит, то соответствующий RLC PDU сегментируется (в отличие от конкатенации) и требует многократной передачи на подуровень MAC для отправки всего протокольного блока.

Логические каналы отображаются (мультиплексируются) в соответствующие транспортные каналы (услуги физического уровня Ph), формируемые физическим уровнем Ph [6-8], т. е. физический уровень предоставляет услуги уровню MAC в форме транспортных каналов. Транспортный канал определяет, как и с какими характеристиками (модуляция, антенны и пр.) происходит передача информации по радио интерфейсу. Физический уровень выполняет функции кодирование, скремблирование, мультиплексирование TB MAC в радиокадр (протокольный блок физического уровня Ph) и модуляцию, для дальнейшей передачи по радио интерфейсу в физических каналах. Транспортные блоки MAC на физическом уровне размещаются в субкадрах. Одна из основных услуг, предоставляемых транспортным каналом Ph, — распределение частотно-временного ресурса в виде ресурсных боков RB (Recourse Block) для каждого соединения на физическом уровне в блоке планирования — субкадре.

Физический уровень Ph планирует транспортные каналы, т. е. производит диспетчеризацию TB MAC (TM, UM или AM) во временной и частотной области субкадров. Каждый частотно-временной ресурс слота содержит свой PCI (TM, UM, AM). То есть, «полезная нагрузка» каждого субкадра определяется числом TB MAC определенной «окраски». Субкадры формируются из группы ресурсных блоков RB вместе со служебной информацией PCI. Передача данных в нисходящей линии связи и восходящей линии связи использует типы транспортных каналов (услуги физического уровня) DL-SCH и UL-SCH соответственно. DL-SCH и UL-SCH являются основными транспортными каналами нисходящей линии связи и восходящей линии связи соответственно. Различие структур в том, что в нисходящем направлении на MAC-подуровне происходит управление приоритетом нескольких UE, в то время как в восходящем направлении такое управление относится только к одному UE. Несколько TB MAC могут быть переданы вместе как по восходящему, так по нисходящему каналу. DL-SCH поддерживает такие особенности LTE, как адаптацию изменения скорости и диспетчеризацию TB MAC во временной и частотной области, HARQ (Hybrid Automatic Repeat request) —- модифицированный автоматический запрос на повторную передачу непринятых пакетов, и пространственное разделение каналов. UL-SCH — Канал с разделением пользователей вверх, аналогичный каналу с разделением пользователей вниз DL-SCH.

В докладе подробно исследуются особенности реализации программной структуры архитектуры сети радиодоступа E-UTRAN в сессии с учетом типа передаваемого трафика в выделенных радиоканалах. Анализируются уровневые протоколы и приводятся форматы и структура уровневых протокольных блоков.

СПИСОК ЛИТЕРАТУРЫ

1. Мошак Н. Н. Особенности архитектуры сети LTE // Волновая электроника и инфокоммуникационные системы: Двадцать третья междунар. науч. конф. СПб., 1-5 июня 2020 г. : сб. статей : в 2 ч. Ч. 2. СПб. : ГУАП, 2020. С. 320-330. (код доступа http://weconfru.guap.ru).
2. Мошак Н. Н. Структурный метод анализа базовых функций архитектур сетей LTE и IMS // Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет ; науч. ред. Б..В. Соколов. Севастополь : СевГУ, 2021. 201 с. ISBN 978-5-6044481-1-3. С. 26-37
3. 3GPP TS 36.323 E-UTRA: спецификация протокола конвергенции пакетных данных (PDCP). URL: https://www.atis.org/wp-content/uploads/3gpp-documents/Rel99-14/ATIS.3GPP.36.323V1120-2013.pdf (дата обращения: 01.10.2023).
4. 3GPP TS 36.322 E-UTRA: спецификация протокола управления радиоканалом (RLC). URL: https://www.atis.org/wp-content/uploads/3gpp-

documents/Rel16/ATIS.3GPP.36.322.V1600.pdf (дата обращения: 01.10.2023).
5. 3GPP TS 36.321 E-UTRA: спецификация протокола управления доступом (MAC). URL: https://www.atis.org/wp-content/uploads/3gpp-documents/Rel15/ATIS.3GPP.36.321.V1590~0.pdf (дата обращения: 01.10.2023).
6. Physical Channel and Modulation, (Release 8). 3GPP TS 36.201 E-UTRA: физический уровень LTE. Общее описание.
7. 3GPP (2009). Technical specification ts36.211 version 8.7.0 Evolved Universal Terrestrial Radio Access (E-UTRA).
8. Мошак Н. Н., Птицына Л. К. Реализация логической структуры физического уровня сети LTE // Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конф. Севастополь, 22-26 сентября 2020 г. / Севастопольский государственный университет ; науч. ред. Б. В. Соколов. Севастополь : СевГУ, 2020. 305 с. ISBN 978-5-6044481-1-3. С. 61-64. URL: http://pnroit.code-bit.com/.

УДК 621.391.28

IPX НОВАЯ ПАРАДИГМА КОНВЕРГЕНЦИИ МОБИЛЬНЫХ И ФИКСИРОВАННЫХ СЕТЕЙ NGN

Мошак Николай Николаевич, Медведев Дмитрий Сергеевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков, пр., 22, Санкт-Петербург, 193323, Россия
e-mail: nnmoshak49@ mail.ru, ds1000one@gmail.com

Аннотация. Рассматривается схема организации межсетевого конвергентного IP-соединения в фиксированном сценарии мобильного взаимодействия пользователей сетей LTE через операторов IMS и IPX-провайдеров. Исследуются особенности построения сети IPX и механизмы обеспечения качества сервиса QoS сквозной передачи end-to-end трафика различной природы. Приводятся основные достоинства сети IPX.

Ключевые слова: сеть LTE; IP-мультимедийная система IMS; конвергенция фиксированных и мобильных сетей; сеть IPX.

IPX NEW PARADIGM FOR CONVERGENCE OF NGN MOBILE AND FIXED NETWORKS

Moshak Nikolay, Medvedev Dmitry
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bryuevich
Bolsheviks, pr., 22, St. Petersburg, 193323, Russia
e-mail: nnmoshak49 @ mail.ru, ds1000one@gmail.com

Abstract. We are considering a scheme for organizing an Internet converged IP connection in a fixed scenario of mobile interaction between users of LTE networks through IMS operators and IPX providers. The features of building an IPX network and mechanisms for ensuring the quality of QoS service of end-to-end traffic of various nature are investigated. The main advantages of the IPX network are given.

Keywords: LTE network; IP multimedia system IMS; convergence of fixed and mobile networks; IPX network.

Конвергенция фиксированных и мобильных сетей (Fixed and Mobile Convergence, FMC) на архитектуре NGN позволяет операторам предоставлять новые и традиционные услуги с любых терминалов через любую совместимую точку доступа. При этом для пользователей появляется возможность организации «виртуальной домашней среды» (Virtual Home Environment, VHE), т.е. они могут осуществлять роуминг между различными сетями и получать одинаковый набор услуг как в «домашних», так и в «визитных» сетях [1]. В настоящее время IP-мультимедийная система IMS (IP Multimedia Subsystem) рассматривается многими операторами и сервис-провайдерами, а также поставщиками оборудования как возможное решение для построения сетей следующего поколения NGN и как основа конвергенции мобильных и фиксированных сетей FMC на платформе IP. Система IMS строится на архитектуре NGN, обеспечивает реализацию большого числа инфокоммуникационных услуг, а также дает возможность традиционным телефонным операторам, операторам мобильной связи и различным сервис-провайдерам предлагать свои услуги пользователям всех типов сетей доступа и всех типов терминалов через единую транспортную сеть на базе протокола IP-MPLS.

Для решения проблемы обеспечения требуемого уровня качества сервиса QoS на уровне трафика в FMC необходимо введение различных функций, такие как авторизация QoS, схема распределения QoS относительно сервиса и трафика и способы для обеспечения управления QoS. В идеале должно так же учитываться сквозное управление QoS, то есть работу в комбинированных сетях, каналах передачи информации и провайдерах сервиса, которые включают будущие NGN. Традиционно, для голосового трафика между различными операторами использовалась международные стандарты SS7/TDM. Однако в последнее время все IP-парадигмы с VoIP быстро вводятся разными операторами в различных формах, таких как IMS. Для того, чтобы свести к минимуму число преобразований между коммутацией голосовых пакетов и коммутацией голосовых каналов существует явная необходимость в развертывании IP на основе межсетевого интерфейса «сеть-сеть» (Network-to-Network Interface, NNI) и, следовательно, IP, основанном на взаимосвязи сетей.

Новая парадигма в международном межсетевом IP-соединении IP eXchange (IPX), гарантирует сквозное качество обслуживания QoS для нескольких транзитных операторов IMS [3]. IPX — модель телекоммуникационной взаимосвязи для обмена мультимедийным IP-трафиком между пользователями отдельных мобильных (например, LTE) и фиксированных операторов (например, IMS) на основе межсетевого интерфейса NNI [4]. При это IPX требуется только адрес NNI, а интерфейс пользователь-сеть (UNI) не рассматривается. Трафик управляется с помощью уровней QoS и производительности в соответствии с

соглашениями об уровне обслуживания (Service Level Agreement, SLA), которые взаимно согласованы с различными IPX провайдерами и могут регулироваться в зависимости от услуги. При этом сквозная передача end-to-end как сигнальных сообщений (SIP), так и медиа (RTP) передаются в соответствии со спецификацией IPX [3].

IPX - это платформа нового поколения, способная гарантировать высококачественные услуги сквозной передачи медиа и мобильных данных. Благодаря глобальному, безопасному и частному соединению, основанному на IP, решение IPX является наиболее эффективным способом предоставления множества различных услуг в рамках одного конвергентного соединения. Широкое распространение базовых телекоммуникационных сетей на основе IP ведет к смене парадигмы в международном соединении, когда традиционное соединение с временным мультиплексированием TDM между телекоммуникационными сетями заменяется соединением IP. IPX не предназначена для того, чтобы заменить или конкурировать с Интернетом, она предлагает альтернативный вариант для поставщиков услуг. При этом, IPX обеспечивает безопасную IP-среду, которая не взаимодействует с глобальной сетью Интернет. Целью IPX является обеспечение совместимости IP-услуг между всеми видами услуг провайдеров в коммерческой структуре, которая позволяет всем сторонам в цепочке получать коммерческую прибыль. Коммерческие соглашения подкреплены соглашениями об уровне обслуживания SLA, которые гарантируют производительность, качество и безопасность для всех служб и приложений, начиная от обмена медиа до обмена мгновенными сообщениями. Архитектура IPX по своей природе ориентирована на сервисы и обеспечивает безопасное сквозное соединение и качество обслуживания QoS в различных типах сетей поставщиков услуг связи [3].

Провайдер IPX предлагает, как двусторонние, так и многосторонние взаимосвязи. Двусторонняя предполагает традиционную модель, при которой два оператора составляют предварительный контракт о взаимодействии до непосредственной установки соединения друг с другом. Многосторонний же обозначает, что IPX-провайдер обеспечивает соблюдение контракта обеими сторонами и установку соединения от имени операторов. Организация двусторонних договоров о взаимосвязи и подключениях с десятками и сотнями других операторов может быть весьма затруднительной. Поэтому многостороннее взаимодействие, позволяющее оператору открыть несколько соединений, создав единый договор и единую техническую связь с IPX-провайдером, делает взаимодействие проще и быстрее.

В докладе рассматривается схема организации межсетевого конвергентного IP-соединения в фиксированном сценарии мобильного взаимодействия пользователей сетей LTE через операторов IMS и IPX-провайдеров. Исследуются особенности построения сети IPX и механизмы обеспечения качества сервиса QoS сквозной передачи end-to-end трафика различной природы. Приводятся основные достоинства сети IPX.

СПИСОК ЛИТЕРАТУРЫ

1. Н. Н. Мошак. Конвергенция мобильных и фиксированных сетей связи на основе системы IMS // VIII Межрегиональной научно-практической конференции «Перспективные направления развития отечественных информационных технологий (ПНРОИТ-2022)». Севастополь, 20-24 сентября 2022 г. / Севастопольский государственный университет; науч. ред. Б..В. Соколов. – Севастополь: СевГУ, 2022.– 252с. ISBN 978-5-6049992-2-6, 4-7с.
2. Г.Г. Яновский. Статья «IP Multimedia Subsystem: принципы, стандарты и архитектура». 2006г. Вестник связи URL:http://greenmount.narod.ru/qnowskijGG.html (дата обращения 10.10.2023)
3. IP eXchange. URL: https://www.gsma.com/iot/wp-content/uploads/2012/03/ipxbrochure-1.pdf (дата обращения 10.10.2023)
4. VoLTE Service Description and Implementation Guidelines Version 1.1 26 March 2014 [Электронный ресурс] // https://www.gsma.com [сайт]. URL: https://www.gsma.com/futurenetworks/wp-content/uploads/2014/05/FCM.01-v1.1.pdf (дата обращения 10.10.2023).

УДК УДК 004.7

АНАЛИЗ РАСПРЕДЕЛЕННОГО ПЛАНИРОВАНИЯ ДЕЙСТВИЙ В МУЛЬТИАГЕНТНЫХ СИСТЕМАХ

Пелих Дмитрий Александрович, Птицына Лариса Константиновна, Ширин Александр Игоревич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Мойки р. наб., 61, Санкт-Петербург, 191186, Россия
e-mails: elektronstandart@bk.ru, ptitsina_lk@inbox.ru, 1992@mail.ru

Аннотация: Показана востребованность мультиагентных систем в цифровой экономике. Приведены основания для актуальности исследований распределенного планирования мультиагентных систем. Отражена преемственность в знаниях о качестве планирования действий агентов. Описаны ключевые особенности предлагаемого аналитического моделирования распределенного планирования мультиагентных систем.

Ключевые слова: мультиагентная система; действия; планирование; качество; модели; методы; знания.

ANALYSIS OF DISTRIBUTED ACTION PLANNING IN MULTI-AGENT SYSTEMS

Pelikh Dmitry, Ptitsyna Larisa, Shirin Alexander
Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
61 Moika River Emb, St. Petersburg, 191186, Russia
e-mails: elektronstandart@bk.ru, ptitsina_lk@inbox.ru, 1992@mail.ru

Abstract: The demand for multi-agent systems in the digital economy is shown. Reasons for the topicality of research into distributed planning of multi-agent systems are given. Continuity in knowledge about the quality of agent action planning is reflected. The key features of the proposed analytical modeling of distributed planning of multi-agent systems are described.

Keywords: multi-agent system; actions; planning; quality; models; methods; knowledge.

В информационном обществе искусственный интеллект становится областью для национальных стратегий развития цифровой экономики. По мнению специалистов, высшей степенью интеллектуальности обладают артефакты, способные планировать достижение поставленных целей. Мультиагентные системы являются именно теми артефактами, которые обладают подобными возможностями. Благодаря способности достигать поставленных целей, мультиагентные системы находят все большее применение на производстве и транспорте, в здравоохранении, медицине, коммунальном хозяйстве, торговле и во многих иных сферах жизнедеятельности. Востребованность мультиагентных систем предопределяет стремление к повышению качества их функционирования. Непосредственное влияние на качество функционирования оказывает качество планирования действий мультиагентных систем. В силу определяющих особенностей мультиагентных систем планирование их действий относится к разряду распределенного планирования. В этой связи представляемые исследования актуальны в контексте расширения знаний о качестве планирования действий мультиагентных систем.

Предлагаемые расширения опираются на предшествующие знания, связанные с аналитическим моделированием планировщиков действий [1-3]. Для анализа распределенного планирования действий мультиагентных систем разработана методика, предусматривающая построение и преобразование расширенных объектно-ориентированных моделей соответствующих распределенных процессов. Аналитические соотношения, определяющие зависимости плотностей распределения вероятностей времени планирования в каждом субагенте, описают характеристики расширений строящихся моделей. Помимо этих соотношений, в модели вводятся функции, описывающие взаимодействие планировщиков, и характеристики телекоммуникаций. Описание каждого этапа методики сопровождает система взаимосвязанных методов преобразований, приводящих к определению статистических характеристик времени распределенного планирования. Полученные результаты проведенных исследований обеспечивают управляемость качеством распределенного планирования мультиагентных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Птицына Л. К., Дамдинов Б. Б. Расширенное объектно-ориентированное моделирование планировщиков для управления крупно-гранулярными процессами // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI –я Международная научно-техническая и научно-методическая конференция : сб. научных статей в 4 т. СПб. : СПбГУТ, 2022. Т. 2. С. 182-185.
2. Ptitsyna L. K., El Sabayar Shevchenko N., Ptitsyn N. A., Belov M. P. Extending Knowledge Representation System about Planners of Intelligent Information Agents // Proceedings of the International Conference on Information Processes and Systems Development and Quality Assurance IPSQDA-2023. March 22-24, 2023. St. Petersburg Russia 2023. Pp. 113-116.
3. Птицына Л. К., Эль Сабаяр Н., Птицын Н. А., Белов М. П. Развитие методов моделирования планировщиков действий интеллектуальных информационных агентов // XXVI Международная конференция по мягким вычислениям и измерениям (SCM-2023) : сб. докладов. Санкт-Петербург, 24-26 мая 2023 г. СПб. : СПбГЭТУ «ЛЭТИ». С. 58-61.

УДК 004.056.53.

ИССЛЕДОВАНИЕ ИНСТРУМЕНТАРИЯ WEBSPLOIT ДЛЯ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПРОВОДНОЙ СЕТИ

Петрова Татьяна Васильевна, Кузьмина Ольга Ивановна,
Ковцур Максим Михайлович, Кистуруга Антон Юрьевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22, корп. 1, Санкт-Петербург, 193232, Россия
e-mails: tanya26012001@mail.ru, Olgakuzmina2000@mail.ru, maxkovzur@mail.ru, anton.kistruga@gmail.com

Аннотация. В данной статье рассматриваются возможности платформы Websploit, которая предназначена для тестирования веб-приложений и сетей, а также чем данная платформа может помочь при борьбе с различными атаками киберпреступников.

Ключевые слова: Websploit; тестирование веб-приложений и сетей; безопасность беспроводной сети.

THE WEBSPLOIT TOOLKIT FOR WIRELESS NETWORK INFORMATION SECURITY ASSESSMENT

Petrova Tatyana, Kuzmina Olga, Kovzur Maxim, Kistruga Anton
Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: tanya26012001@mail.ru, olgakuzmina2000@mail.ru, maxkovzur@mail.ru, anton.kistruga@gmail.com

Abstract. This article describes capabilities of Websploit platform, which is designed to test web applications and networks, and how this platform can help in the fight against various cybercriminal attacks.

Keywords: Websploit; testing web applications and networks; wireless network security.

Websploit — это фреймворк с открытым исходным кодом, используемый для тестирования на проникновение и этического взлома. Также он предназначен для автоматизации общих задач, выполняемых во время тестирования веб-приложений, таких как снятие отпечатков пальцев, сканирование на наличие уязвимостей и их использование. Данная платформа включает в себя широкий спектр инструментов для различных этапов процесса тестирования на проникновение, таких как сбор информации, сканирование уязвимостей, взлом паролей и отображение сети. Он поддерживает различные платформы и может использоваться как в операционных системах Windows, так и в Linux. Websploit обычно используется специалистами по безопасности, этичными хакерами и тестировщиками на проникновение для выявления и устранения уязвимостей в веб-приложениях.

Также данный интструмент может быть использован для выполнения множества задач в процессе тестирования на проникновение веб-приложений. Некоторые из них включают:

1. Сбор информации: Websploit может использоваться для сбора информации о целевой системе, такой как IP-адреса, открытые порты, используемые операционные системы и технологии веб-сервера [1].
2. Сканирование на уязвимости: Websploit может сканировать веб-приложения на наличие уязвимостей, таких как SQL-инъекции, кросс-сайтовый скриптинг, уязвимости в аутентификации и авторизации и другие.
3. Эксплуатация уязвимостей: Websploit может использоваться для эксплуатации обнаруженных уязвимостей в веб-приложениях, например, для получения удаленного доступа к серверу или для выполнения команд на удаленном хосте.
4. Взлом паролей: Websploit может использоваться для взлома паролей, как локально, так и удаленно, используя различные методы, такие как словарь атаки, атака брутфорсом и другие.
5. Картирование сети: Websploit может использоваться для картирования сети, чтобы определить структуру сети и обнаружить уязвимые узлы.

В целом, Websploit является мощным инструментом для тестирования на проникновение веб-приложений, который может помочь в обнаружении и устранении уязвимостей в системе. Однако, следует помнить, что использование данного инструмента для атаки на системы без разрешения владельца является незаконным.

Websploit также может использоваться для проведения атак на беспроводные сети [2, 3]. Некоторые из возможных атак включают:

1. Атака на WEP: Websploit может использоваться для проведения атак на сети, защищенные протоколом WEP, и получения доступа к зашифрованным данным.
2. Атака на WPA/WPA2: Websploit может использоваться для проведения атак на сети, защищенные протоколами WPA и WPA2, и получения доступа к зашифрованным данным.
3. Атака на точки доступа: Websploit может использоваться для проведения атак на точки доступа и получения доступа к защищенным сетям, подключенным к этим точкам доступа [4].
4. Атака на клиентов: Websploit может использоваться для проведения атак на клиентов беспроводных сетей и получения доступа к их устройствам и данным.
5. Атака на Bluetooth: Websploit может использоваться для проведения атак на Bluetooth-устройства и получения доступа к их данным и функциям.

СПИСОК ЛИТЕРАТУРЫ

1. Ковцур М. М., Герлинг Е. Ю., Коновалова В. В., Киструга А. Ю. Исследование способов удаленного перехвата трафика в корпоративных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 68-75.
2. Александрова Е. С., Ковцур М. М. Разработка модели нарушителя в беспроводных сетях стандарта IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 2. С. 24–28.
3. Александрова Е. С., Иванов Г. Н., Ковцур М. М. Анализ механизмов защиты Wi-Fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 47-51.
4. Красов А. В., Петрив Р. Б., Сахаров Д. В., Сторожук Н. Л., Ушаков И. А. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 86-97.

УДК 004.7

ОНТОЛОГИЯ АРХИТЕКТУРЫ ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ПРОГНОЗА БИРЖЕВЫХ КОТИРОВОК

Птицын Никита Алексеевич, Птицына Лариса Константиновна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Мойки р. наб., 61, Санкт-Петербург, 191186, Россия
e-mails: nikita_pti@inbox.ru, ptitsina_lk@inbox.ru

Аннотация: Рассмотрены причинно-следственные связи ключевых направлений развития цифровой экономики, искусственного интеллекта и информационных систем прогноза биржевых котировок. Показана перспективность расширения жизненного цикла интеллектуальных информационных систем прогноза биржевых котировок. Раскрыт контент расширения за счет введения этапа онтологического проектирования архитектуры. Описаны основные теоретико-множественные формализации онтологического проектирования архитектуры интеллектуальных информационных систем прогноза биржевых котировок. Представлена технологическая основа разработки онтологий архитектур рассматриваемых систем. Выделены преимущества предлагаемых инновационных компонентов жизненного цикла интеллектуальных информационных систем прогноза биржевых котировок.

Ключевые слова: информационная система; котировки; архитектура; жизненный цикл; онтологическое проектирование.

ONTOLOGY OF ARCHITECTURE OF INTELLIGENT INFORMATION SYSTEMS FOR FORECASTING STOCK QUOTES

Ptitsyn Nikita, Ptitsyna Larisa
Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
61 Moika River Emb, St. Petersburg, 191186, Russia
e-mails: nikita_pti@inbox.ru, ptitsina_lk@inbox.ru

Abstract. The cause-and-effect relationships of key areas of development of the digital economy, artificial intelligence and information systems for forecasting stock quotes are considered. The prospects for expanding the life cycle of intelligent information systems for forecasting stock quotes are shown. The content of the extension is revealed by introducing the stage of ontological design of architecture. The main set-theoretic formalizations of the ontological design of the architecture of intelligent information systems for forecasting stock quotes are described. The technological basis for the development of ontologies of the architectures of the systems under consideration is presented. The advantages of the proposed innovative components of the life cycle of intelligent information systems for forecasting stock quotes are highlighted.

Keywords: information system; quotes; architecture; life cycle; ontological design.

Магистральными направлениями развития цифровой экономики предусматривается повышение конкурентоспособности отечественных субъектов хозяйствования в рыночных отношениях при различных условиях в окружающей обстановке. Подобным целеполаганием предопределяется востребованность анализа поведения показателей биржевых котировок. Актуальность автоматизации анализа поведения показателей биржевых котировок проявляется в разнообразии постановок задач исследований, направленных на повышение качества обнаружения изменений в прогнозе и его точности [1-7]. При этом открытыми остаются архитектурные контексты информационных систем прогноза биржевых котировок. В то же время анализ больших данных, проводимый при прогнозировании биржевых котировок, остро нуждается в создании и применении интеллектуальных информационных систем рассматриваемого назначения, эффективно использующих технологии искусственного интеллекта.

Современный теоретический и практический задел в области разработки и применения интеллектуальных информационных технологий позволяет формализовать представление жизненного цикла информационных систем прогноза биржевых котировок, начиная с разработки парадигмы их архитектуры. С позиций теории искусственного интеллекта разработка парадигмы архитектуры выполняется на основе онтологического подхода. В связи с этим предлагается расширение жизненного цикла информационных систем прогноза биржевых котировок посредством введения этапа онтологического проектирования их архитектуры.

При разработке парадигмы архитектуры интеллектуальных информационных систем прогноза биржевых котировок предусматриваются вариации:

- в требованиях к системам;
- в свойствах систем;
- в условиях применения систем;
- в критериях и показателях качества функционирования систем;
- в моделях описания доступных больших данных;
- в моделях поведения биржевых котировок;
- в методах прогнозирования, основанных на обработке структурированной информации о поведении биржевых котировок;
- в методах прогнозирования, ориентированных на обработку представлений слабоструктурированной информации о поведении биржевых котировок;
- в методах раннего обнаружения изменений в прогнозах;
- в ресурсах, выделяемых для создания систем;
- в технологиях доступа к большим данным;
- в вычислительных технологиях обработки больших данных;
- в технологиях программирования;
- в режимах работы систем;
- в информационной безопасности систем;
- в методах генерации модельно-аналитического интеллекта систем, оценивающего качество прогнозирования;
- в методах генерации модельно-аналитического интеллекта систем, оценивающего качество функционирования систем;
- в режимах использования модельно-аналитического интеллекта систем;
- в организации процессов управления качеством прогнозирования биржевых котировок.

Представленные вариации детализируются при теоретико-множественном описании парадигмы архитектуры интеллектуальных информационных систем прогноза биржевых котировок.

Вследствие многообразия вариаций образуется многоуровневая онтология, описывающая парадигму архитектуры интеллектуальных информационных систем прогноза биржевых котировок. На каждом из уровней сохраняется однородность типа вариации.

Онтология архитектуры интеллектуальных информационных систем прогноза биржевых котировок порождает множество соответствующих концепций, каждая из которых согласуется с требованиями, актуальными для окружающей среды и текущих условий профессиональной деятельности. Индустриальный подход к расширению жизненного цикла проектирования интеллектуальных информационных систем прогноза биржевых котировок обеспечивается применением современных сред онтологического проектирования. Предпочтение отдается тем средам, в которых поддерживается верификация на непротиворечивость.

Раскрытие предлагаемых инноваций в жизненном цикле интеллектуальных информационных систем прогноза биржевых котировок осуществляется с применением среды Protégé.

Научная новизна выполненных исследований заключается:

– в формализации процесса разработки парадигмы архитектуры интеллектуальных информационных систем для прогноза биржевых котировок на основе онтологического подхода;

– в определении типа многоуровневости онтологии архитектуры интеллектуальных информационных систем для прогноза биржевых котировок;

– в генерации множества концепций создания интеллектуальных информационных систем для прогноза биржевых котировок;

– в сквозном связывании технологий интеллектуальных информационных систем для прогноза биржевых котировок.

Практическая значимость предопределяется:

– расширением технологических возможностей интеллектуальных информационных систем для прогноза биржевых котировок;

– управляемостью качеством прогнозирования биржевых котировок в соответствии с актуальными требованиями.

СПИСОК ЛИТЕРАТУРЫ

1. Птицына Л. К., Птицын Н. А. Расширение знаний о раннем обнаружении появляющихся изменений // Наука. Информатизация. Технологии. Образование. Материалы XIII международной научно-практической конференции «Новые информационные технологии в образовании и науке НИТО 2020» 24–28 февраля 2020 г. г. Екатеринбург / ФГАОУ ВО «Российский государственный профессионально-педагогический университет». Екатеринбург, 2020. С. 248-252.
2. Нильсен Э. Практический анализ временных рядов : прогнозирование со статистикой и машинное обучение : перевод с английского / Эйлин Нильсен. Москва ; Санкт-Петербург : Диалектика, 2021. 538 с.
3. Птицын Н. А. Птицына Л. К. Автоматическое отслеживание изменений показателей профессиональной деятельности // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2022). Всероссийская научно-методическая конференция магистрантов и их руководителей : Сборник лучших докладов конф. СПб. : СПбГУТ, 2023. С. 343-347.
4. Артамонов Н. В., Ивин Е. А., Курбацкий А. Н., Фантаццини Д. Введение в анализ временных рядов : учеб пособие для вузов. Вологда : ВолНЦ РАН, 2021. 134 с.
5. Прогнозирование котировок фьючерсов на индекс РТС на основе машинного обучения / Воинов Н. В. [и др.] // Материалы международной конференции по мягким вычислениям и измерениям. Т. 1. 2021. С. 271–274.
6. Дорошенко С. Н., Прийма К. А., Ляшенко А. Я. Анализ рынка акций на примере российских горнодобывающих компаний // Актуальные проблемы экономики и управления. 2022. № 1 (33). С. 3-7.
7. Французенко П. С. Исследование изменений индекса Мосбиржи в зависимости от количества зарегистрированных пользователей // Вестник Академии знаний. 2022. № 48 (1). С. 461-466.

УДК 004.7

МИКРОСЕРВИСЫ ПОВЫШЕНИЯ КАЧЕСТВА ПОИСКА ИНФОРМАЦИИ

Птицына Лариса Константиновна, Солтык Алексей Михайлович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Мойки реки наб., 61, Санкт-Петербург, 191186, Россия
e-mails: ptitsina_lk@inbox.ru, seo.soltyk@yandex.ru

Аннотация. Рассмотрены основания для развития технологий повышения качества поиска информации. Выявлена актуальность объединения различных подходов к повышению качества поиска информации. Показана перспективность интеграции компонентов технологий повышения качества поиска информации с применением сервис-ориентированной архитектуры. Предложена микросервисная система для повышения качества поиска информации. Представлены разработанные и исследованные образующие микросервисы.

Ключевые слова: информация; поиск; качество; система; интеграция; микросервисы.

MICROSERVICES TO IMPROVE THE QUALITY OF INFORMATION SEARCH

Ptitsyna Larisa, Soltyk Alexey
Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich,
61 Moika River Emb, St. Petersburg, 191186, Russia
e-mails: ptitsina_lk@inbox.ru, seo.soltyk@yandex.ru

Abstract. The grounds for the development of technologies for improving the quality of information retrieval are considered. The relevance of combining different approaches to improve the quality of information retrieval is revealed. The prospects of integrating components of technologies for improving the quality of information retrieval using a service-oriented architecture are shown. A microservice system is proposed to improve the quality of information retrieval. The developed and researched generating microservices are presented.

Keywords: information; search; quality; system; integration; microservices.

В информационном обществе поиск информации становится непременным спутником жизнедеятельности. При цифровой трансформации поиск информации включается в жизненный цикл любого артефакта.

Ключевые технологические причины проблемной ситуации, связанной с поиском информации, обуславливаются отличиями представления пользовательского поискового запроса от способа его интерпретации. Субъект руководствуется семантическими единицами, а термины запроса для поисковых машин анализируются как синтаксические единицы. Выявленная ситуация является одной из основных причин ограниченности релевантности. В связи с этим уделяется много внимания на развитие технологий поиска информации [1-4].

Обширный спектр современных подходов к повышению поиска информации представляется перспективным к объединению на системном уровне. Подобное объединение удается организовать при использовании сервис-ориентированной архитектуры многокомпонентного программного обеспечения.

В представляемом исследовании разрабатывается и анализируется микросервисная система для повышения качества поиска информации. Исследование проводится на использовании теории сложных систем, методов теории информационных систем, теории вероятностей и математической статистики, методов веб-технологий.

В микросервисной системе интегрируются микросервис кластеризации поисковых запросов, микросервис конкурентного анализа, микросервис анализа текстовых данных, микросервис по массовой проверке типа микроразметки, микросервис по проверке позиций сайта в поисковых системах, микросервис по оценке конкурентности поисковых запросов на основе показателя Яндекс ИКС.

Процесс взаимодействия между микросервисами реализуется посредством применения RESTful API и протокола HTTP.

Научная новизна выполненных исследований заключается в расширении архитектур сервис-ориентированных систем для повышения качества поиска информации, сопровождающего различные сферы деятельности.

Практическую значимость представляет возможность использования разработанной системы для рационализации контента сайта и повышения его значимости в поисковых системах.

СПИСОК ЛИТЕРАТУРЫ

1. Ли Х., Чен Л. Исследование тенденций развития технологий поисковых систем // 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). 2018. С. 2239-2243.
2. Сазонов М. А., Яковлев А. В., Кожанчиков М. О., Мазниченко А. А. Разработка перспективных методов поиска и классификации текстовой информации из открытых источников сети Интернет // Системы управления и информационные технологии. 2023. № 2 (92). С. 92-95.
3. Сакулин С. А., Алфимцев А. Н., Недашковский В. М., Кальгин Ю. А. Повышение эффективности поиска информации в Интернете на основе формирования метакогнитивной стратегии // Вестник компьютерных и информационных технологи. 2022. Т. 19. № 1 (211). С. 26-36.
4. Скубиро К. В., Воронин В. В. Тенденции развития алгоритмов оиска информации в Интернете и социальных сетях // Информационные технологии XXI века : сборник научных трудов. Х., 2023. С. 172-175.

УДК 004.492.2

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ НА ОСНОВЕ ИММУНОКОМПЬЮТИНГА

Тюменцев Алексей Андреевич, Бондаренко Игорь Борисович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: zscauer@gmail.com, ius@sut.ru

Аннотация. Рассматривается возможность эффективного применения алгоритмов на основе иммунокомпьютинга для повышения уровня защищенности информационной сети от угроз проникновения.

Ключевые слова: вторжения, иммунокомпьютинг, информация, иммунные сети.

INTRUSION DETECTION BASED ON IMMUNOCOMPUTING

Tyumentsev Aleksey, Bondarenko Igor
Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
email: zscauer@gmail.com, ius@sut.ru

Abstract. Considering the possibility of effective application of algorithms based on immunocomputing for increasing the level of information network security against intrusions threats.

Keywords: intrusions; immunocomputing, information, immune network.

Мы живем в информационную эпоху, в которой ключевую роль играет информация и ее обмен. Современное общество трансформировалось таким образом, что информация становится критически важной для его нормального функционирования. На информацию опираются практически все службы — правоохранительные органы используют данные с видеокамер и социальных сетей для обнаружения злоумышленников/предотвращения правонарушений, органы здравоохранения опираются на информацию о прошлых состояниях пациента при установке диагноза и т.д.

Так как общественные институты тесно связаны между собой, можно рассматривать их как единую систему, в которой общее состояние зависит от функционирования каждой его части, подобно человеческому организму, и так же, как и человеческий организм, общество нуждается в защите всех его частей. В организме человека существует механизм по обнаружению новых, не известных ранее угроз, с целью их устранения — иммунитет. В мире, где новые угрозы для информационной безопасности появляются ежедневно, со все большей скоростью, необходим аналогичный инструмент, который мог бы действовать на опережение.

В иммунной системе живого организма задача информационной целостности клетки решается средствами самой клетки (дублирование информации, защитные свойства мембраны, включение апоптоза и т.п.), а также средствами ИмС, а именно, проверкой с помощью системы комплемента и различных типов лейкоцитов признаков принадлежности данной клетки родительскому организму. Для этого используется, как на современных самолетах, не сложный, но секретный прибор «свой-чужой». С большой вероятностью можно сказать, что в основе алгоритма данного прибора лежит уникальный для данного организма код ДНК, которым обладает, как контролируемая так контролирующая клетки. Генная библиотека искусственной иммунной системы должна содержать «гены» (это могут быть, например, данные о характерном количестве пакетов, их длине, структуре, типичных ошибках и т.д.), на основании которых будут генерироваться особые программные агенты — детекторы, служащие аналогами лимфоцитов.

Подобные механизмы, опирающиеся на принципы работы иммунитета, легли в основу относительно нового направления в информатике — иммунокомпьютинга [1-3].

Иммунокомпьютинг (ИК) представляет собой новое направление информатики, базирующееся на принципах обработки информации молекулами белков и иммунными сетями [1]. ИК ведет к разработке компьютера нового типа, который предложено назвать иммунокомпьютером по аналогии с известными нейрокомпьютерами, которые аппаратно реализуют модели нейрона и нейронной сети.

С ИК связаны три основных инновации:

1. Новый математический базис;
2. Новый тип вычислений;
3. Новый тип аппаратной реализации.

В связи с ростом значимости информации, важностью стабильной работы информационных систем для полноценного функционирования современного общества и непрерывным ростом возможных угроз информационной безопасности, с другой стороны, является важным рассмотреть возможность эффективного применения системы на основе иммунокомпьютинга для обеспечения безопасности информационной сети благодаря обнаружению вторжений, обладающих характеристиками, отличающимися от уже известных.

СПИСОК ЛИТЕРАТУРЫ

1. Тараканов А. О. Иммунокомпьютинг — биочип — биокомпьютер. СПб. : СПИИРАН, 2002. 104 с.
2. Иммунокомпьютинг // Хакер :журнал. 2006. [Электронный ресурс]. URL:https://xakep.ru/2006/06/16/32265/ (дата обращения: 17.06.2023).
3. Блюм В. С. Иммунная система и иммунокомпьютинг. СПб. : СПИИРАН, 2008. С. 9–13.

УДК 004.056

ПРИМЕНЕНИЕ ТЕОРИИ БИФУРКАЦИЙ ДЛЯ АНАЛИЗА КИБЕРБЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Шашкин Владислав Сергеевич[1], Петрова Татьяна Сергеевна[1], Бирих Эрнест Владимирович[1], Сахаров Дмитрий Владимирович[1,2], Липатников Валерий Алексеевич[2]

[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия

[2] Военная академия связи имени Маршала Советского Союза С. М. Буденного Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e–mails: vlad_shash@mail.ru, be1982@mail.ru, 9992125013@mail.ru, lipatnikovanl@mail.ru, sguard7@mail.ru

Аннотация. В контексте развития информационной безопасности в настоящее время практически не используется методология теории бифуркаций. Многообразие научных областей, применяющих знания указанной теории, позволяет предположить возможность ее использования при изучении динамики кибернетических атак, а также смоделировать противодействие нарушителя и защитника информационной системы в зависимости от определенных условий и ситуаций. В данном исследовании результат бифуркационного перехода представлен с точки зрения возможности получения нарушителем охраняемых сведений конфиденциального характера при атаке на объекты критической инфраструктуры вследствие ветвления потенциального развития событий. Целью исследования является определение допустимости использования теории бифуркаций для анализа защищенности объектов критической инфраструктуры.

Ключевые слова: информационная безопасность; критическая инфраструктура; кибербезопасность; кибернетическая атака; атакующий объект; модель нарушителя; теория бифуркаций; точка бифуркации.

APPLICATION OF THE THEORY OF BIFURCATIONS FOR THE ANALYSIS OF CYBER SECURITY OF OBJECTS OF CRITICAL INFRASTRUCTURE

Shashkin Vladislav[1], Petrova Tatiana[1], Birikh Ernest[1], Sakharov Dmitrii[1,2], Lipatnikov Valery[2]

[1] Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia

[2]The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
Tikhoretsky Av, St. Petersburg, 194064, Russia

e–mails: vlad_shash@mail.ru, be1982@mail.ru, 9992125013@mail.ru, lipatnikovanl@mail.ru, sguard7@mail.ru

Abstract. In the context of the development of information security, the methodology of the theory of bifurcations is practically not used at present. The variety of scientific fields that apply the knowledge of this theory makes it possible to equally assume the possibility of its use in studying the dynamics of cybernetic attacks, as well as to simulate the counteraction of the violator and the defender of the information system, depending on certain conditions and situations. In this study, the result of a bifurcation transition is presented from the point of view of the possibility for an intruder to obtain protected information of a confidential nature during an attack on critical infrastructure objects due to the branching of a potential development of events. The purpose of the study is to determine the admissibility of using the theory of bifurcations to analyze the security of critical infrastructure objects.

Keywords: information security; critical infrastructure; cybersecurity; cyber-attack; attacking object; intruder model; bifurcation theory; bifurcation point.

Идентификация источников угроз, планирование действий нарушителя, комплексы активного противодействия противнику и оценка вероятного ущерба являются известными практиками в сфере кибербезопасности. Проводятся исследования, позволяющие выявить закономерности, построить алгоритмы, модели и системы с целью использования наиболее эффективных оборонительных тактик и ответных наступательных мер, ведущихся в условиях кибернетического противоборства [1-2]. При этом используется апробированный математический аппарат (теория вероятностей, аппарат Марковских процессов, теория графов и другой) [3, 4]. В то же время, в различных моделируемых динамических процессах в состоянии безопасности информационно-телекоммуникационных систем наступают выраженные переломные кризисные события, описанные в теории бифуркаций, что свидетельствует о возможности ее прикладного использования. В связи с этим целью исследования является определение допустимости использования теории бифуркаций для анализа защищенности объектов критической инфраструктуры и выработки упреждающих мер противодействия.

Теория бифуркаций динамических систем описывает качественные, скачкообразные изменения фазовых портретов дифференциальных уравнений при непрерывном, плавном изменении параметров. При этом понятие динамической системы обобщенно включает объекты и процессы кибернетики, состояние которых задается законом эволюции и описывается системами дифференциальных уравнений, алгоритмами и другими способами. Более того, бифуркации одного и того же типа возникают и в простых, и в сложных нелинейных системах [5].

Здесь следует отметить, что в рамках данного исследования особый интерес представляет понятие точки бифуркации. При нахождении системы около точки бифуркации — флуктуации усиливаются при малых изменениях начальных данных. В окрестности этих точек бифуркация изменяет устойчивость. В этом случае параметр α переходит через значение $\alpha = \alpha_1$. Стабильно ветвь устойчивость теряет, неустойчивая — приобретает. Бифуркация является своеобразной складкой.

Во втором случае при нахождении $\alpha = \alpha_{2,3}$ положение равновесия изолируется, затем исчезает или разветвляется на два новых — устойчивое и неустойчивое.

Третий тип бифуркации встречается при вилке функций *f*. Смена характера устойчивости ветви кривой равновесий происходит в точке бифуркации. От нее ответвляются две вновь возникшие ветви с противоположным характером устойчивости [6].

В кибербезопасности динамическая система представляет собой совокупность объектов и связей между ними, а именно, атаку, атакующего, атакуемого объекта, его уязвимостей, а также целей атаки [7, 8]. Нарушитель пытается изменить атакуемый объект. В этом варианте точкой бифуркации является успешная атака нарушителя, приводящая к потере устойчивости системы и резкому выходу из состояния равновесия, а бифуркационным переходом — ветвление системной траектории и потенциальных состояний. Однако на основе риск-ориентированного подхода в целях защиты от вторжения следует комплексно рассматривать способы возможного воздействия злоумышленника на защищаемые ресурсы и объекты, обоснованно использовать процессный подход для управления информационной безопасностью [9, 10]. С применением теории бифуркаций также возможны стратегии снижения последствий воздействия вирусных атак в случае, если эффективность контрмер выше скорости распространения вируса в системе [11, 12]. Данный пример является упрощенным, поскольку количество объектов, алгоритмов и связей между ними в реальности усложнит интерпретацию.

На основании полученных и имеющихся результатов, сделан вывод: кибернетическая система может быть корректно рассмотрена в контексте теории бифуркации исходя из данных о характеристиках метрик для классификации целей и признаков атак, а также на основе взаимосвязей объектов безопасности. Изменение

параметров модели нарушителем вызывает потерю стабильности. В этой связи принципиальное значение приобретает эффективный контроль защитником динамики процесса, направленный на поддержание системы в окрестностях точек бифуркации. При удачной атаке, направленной на такие объекты, как люди, документы и технические средства систем обработки данных, злоумышленник получает несанкционированный доступ к сведениям конфиденциального характера, после чего система попадает в неустойчивую зону. Бифуркационный сценарий процесса фазового перехода системы из одного состояния в другое зависит от вариативности связей причины и следствия и моделируется только в том случае, если возможные угрозы кибератак распознаны и проанализированы.

Таким образом, применение теории бифуркаций может быть положено в основу анализа защищенности объектов критической инфраструктуры.

Работа выполнена при финансовой поддержке «Гранта ИБ МТУСИ» 2022 г. № 10/22-к.

СПИСОК ЛИТЕРАТУРЫ

1. Бирих Э. В., Сахаров Д. В. Модель нарушителя распределенной информационно-вычислительной сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании : сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 235-238.
2. Костарев С. В., Карганов В. В., Липатников В. А. Технологии защиты информации в условиях кибернетического противоборства : монография. СПб: Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи им. Маршала Советского Союза С. М. Буденного» Министерства Обороны Российской Федерации, 2020. 716 с.
3. Кузнецов И. А., Липатников В. А., Сахаров Д. В. Управление АСМК организации интегрированной структуры с прогнозированием состояния информационной безопасности // Электросвязь. 2016. № 3. С. 28-36.
4. Костарев С. В., Липатников В. А., Сахаров Д. В. Модель процесса передачи результатов аудита и контроля в автоматизированной системе менеджмента предприятия интегрированной структуры // Проблемы информационной безопасности. Компьютерные системы. 2015. № 2. С. 120-125.
5. Арнольд В. И., Афраймович В. С, Ильяшенко Ю. С, Шильников Л. И. Теория бифуркаций. Динамические системы. Т. 1. М.: Наука, 1986. С. 5-218.
6. Фомичев А. В.,. Элементы теории бифуркаций и динамических систем. Часть 1 : учеб.-метод. пособие по курсу Аналитическая механика М.: МФТИ, 2019. 42 с.
7. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности : учеб. пособие. СПб: СПб ГУТ, 2012.
8. Сахаров Д. В., Ковцур М. М., Бахтин Д. В. Модель защиты от эксплойтов и руткитов с последующим анализом и оценкой инцидентов // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 22-31.
9. Пиховкин Н. Л., Сахаров Д. В. Обеспечение безопасности распределенной информационно-вычислительной сети с учетом управления рисками // Труды учебных заведений связи. 2016. Т. 2. № 2. С. 93-97.
10. Бухарин В. В., Липатников В. А., Сахаров Д. В. Метод управления информационной безопасностью на основе процессного подхода // Информационные системы и технологии. 2013. № 3 (77). С. 102-109.
11. Липатников В. А., Сахаров Д. В., Кузнецов И. А. Управление безопасностью распределенной ИВС на основе прогноза заражения компьютерным вирусом // Электросвязь. 2017. № 1. С. 53-59.
12. Сахаров Д. В., Штеренберг С. И., Левин М. В., Колесникова Ю. А Разработка модели обеспечения отказоустойчивости сети передачи данных // Известия высших учебных заведений. Технология легкой промышленности. 2016. Т. 34. № 4. С. 14-20.

ОГЛАВЛЕНИЕ

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ 16

ОЦЕНКА РИСКОВ ПРИ РЕГИОНАЛЬНОМ УПРАВЛЕНИИ
Булдакова Татьяна Ивановна, Джалолов Ахмад Шарофиддинович 16

КИБЕРБЕЗОПАСНОСТЬ И СМЕЖНЫЕ ПОНЯТИЯ. НАУЧНО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ В УСЛОВИЯХ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА
Жигадло Валентин Эдуардович 17

СВОБОДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И БЕЗОПАСНОСТЬ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ
Карпов Роман Дмитриевич 19

МЕТОДОЛОГИЯ И ТЕХНОЛОГИИ ПРОАКТИВНОГО УПРАВЛЕНИЯ МОДЕРНИЗАЦИЕЙ КАТАСТРОФОУСТОЙЧИВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
Охтилев Михаил Юрьевич, Соколов Борис Владимирович, Юсупов Рафаэль Мидхатович 21

ОСНОВЫ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ПО ОБНАРУЖЕНИЮ, ПРЕДУПРЕЖДЕНИЮ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕАГИРОВАНИЮ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ
Сторожик Виктор Сергеевич 23

РАЗВИТИЕ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ИНТЕРЕСАХ ПРОМЫШЛЕННОСТИ В РОССИЙСКОЙ АРКТИКЕ
Митько Арсений Валерьевич, Сидоров Владимир Константинович 25

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 28

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ. ИСТОЧНИКИ ВОЗНИКНОВЕНИЯ, СРЕДСТВА И СПОСОБЫ ЗАЩИТЫ
Васютина Татьяна Львовна, Файзулин Алмаз Ильдарович 28

СИСТЕМА УПРАВЛЕНИЯ ЭЛЕКТРОННЫМИ КУРСАМИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ
Воронов Сергей Алексеевич, Примакин Алексей Иванович 29

ГОСУДАРСТВЕННОЕ ГАРАНТИРОВАНИЕ ПРАВ И СВОБОД ЛИЧНОСТИ, ПРАВОВЫЕ АСПЕКТЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ
Громова Ольга Владимировна 31

ПРИМЕНЕНИЕ АЛГОРИТМОВ ФАКТОРНОГО И ДИСПЕРСИОННОГО АНАЛИЗОВ ДЛЯ ФОРМИРОВАНИЯ И ВЫЯВЛЕНИЯ ПРИОРИТЕТНЫХ ФАКТОРОВ, ОПРЕДЕЛЯЮЩИХ УРОВЕНЬ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ПОДРАЗДЕЛЕНИЯХ СИЛОВЫХ СТРУКТУР
Ефимова Анна Борисовна, Примакин Алексей Иванович 34

ПРИМЕНЕНИЕ ТЕОРИИ ИГР ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОДРАЗДЕЛЕНИЯХ РОСГВАРДИИ
Ефимова Анна Борисовна, Примакин Алексей Иванович 35

О НЕОБХОДИМОСТИ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ПОДГОТОВКИ БУДУЩИХ ОФИЦЕРОВ РОСГВАРДИИ ДЛЯ РЕШЕНИЯ ЗАДАЧ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ЗАЩИТЫ НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ РОССИИ
Зозулин Игорь Николаевич, Примакин Алексей Иванович 36

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОБЪЕКТЕ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ
Локнов Алексей Игоревич, Симакова Екатерина Андреевна 37

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВЕДОМСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
Лопатин Богдан Владиславович, Якушев Денис Игоревич 39

ЗАЩИТА ДАННЫХ В ЦИФРОВОЙ ЭПОХЕ
Милованов Андрей Сергеевич, Шалагинова Ольга Борисовна 40

ПУТИ ЗАЩИТЫ И МЕРЫ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЕ ЗАКОНА О ПЕРСОНАЛЬНЫХ ДАННЫХ
Парфенов Николай Петрович, Шалагинова Ольга Борисовна, Карпов Павел Евгеньевич 42

ФОРМИРОВАНИЕ СИСТЕМЫ ПОКАЗАТЕЛЕЙ, ОПРЕДЕЛЯЮЩИХ СТЕПЕНЬ ЗАЩИТЫ ИНФОРМАЦИИ СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ РОСГВАРДИИ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА
Потапова Людмила Сергеевна, Примакин Алексей Иванович 43

АНАЛИЗ УГРОЗ КИБЕРБЕЗОПАСНОСТИ В ОБЛАСТИ ЗДРАВООХРАНЕНИЯ
Пронский Александр Юрьевич, Шалагинова Ольга Борисовна 44

ОБ АСПЕКТАХ ПРИМЕНЕНИЯ НЕКРИМИНАЛИСТИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ
Проурзина Ольга Юрьевна 46

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК МЕРА ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ ОВД
Рогова Юлия Николаевна, Якушев Денис Игоревич 48

ПРАВОВОЕ ОБОСНОВАНИЕ РОЛИ И МЕСТА ПОЖАРНОЙ БЕЗОПАСНОСТИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Синещук Юрий Иванович, Терёхин Сергей Николаевич, Шидловский Григорий Леонидович 50

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ ПРЕДУПРЕЖДЕНИЯ КОРРУПЦИОННЫХ ПРЕСТУПЛЕНИЙ
Синещук Юрий Иванович, Локнов Алексей Игоревич 51

ИНФОРМАТИЗАЦИЯ БИБЛИОТЕК КАК КЛЮЧЕВОЕ НАПРАВЛЕНИЕ ГОСУДАРСТВЕННОЙ БИБЛИОТЕЧНОЙ ПОЛИТИКИ РОССИИ
Стахно Роман Евгеньевич 52

ИНФОРМАЦОННО-АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ В ВОЕННОМ ДЕЛЕ
Шалагинова Ольга Борисовна 54

МАТЕМАТИКА В БОРЬБЕ С ПРЕСТУПНОСТЬЮ
Шалагинова Ольга Борисовна 55

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО БЛАГОПОЛУЧИЯ ЛИЧНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ
Шилков Владимир Ильич 56

СПОСОБ ОЦЕНКИ УРОВНЯ ИСХОДНОЙ ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ЛИЧНЫХ ДАННЫХ
Яковлева Наталья Александровна, Большакова Людмила Валентиновна, Сибаров Константин Дмитриевич, Карпов Павел Евгеньевич 58

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА
ДЛЯ ХРАНЕНИЯ ИНФОРМАЦИИ В ДЕЯТЕЛЬНОСТИ ОВД
Якушев Денис Игоревич, Бушманов Никита Андреевич 59

ОБОСНОВАНИЕ НЕОБХОДИМОСТИ СОВЕРШЕНСТВОВАНИЯ МЕТОДОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ВЕДОМСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ
Якушев Денис Игоревич, Жалдак Анастасия Алексеевна 61

ГРУППОВАЯ ПОЛИТИКА БЕЗОПАСНОСТИ КАК СПОСОБ ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ
Якушев Денис Игоревич, Лукина Ксения Сергеевна 64

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 67

ПРОБЛЕМА БЕЗОПАСНОСТИ ПРИ СБОРЕ, ХРАНЕНИИ И ИСПОЛЬЗОВАНИИ ДАННЫХ ПРИ РАБОТЕ С ЦИФРОВЫМИ ДВОЙНИКАМИ ЛЮДЕЙ
Ананьева Варвара Яновна 67

МОДЕЛЬ ВЫРАБОТКИ РЕСУРСА ТВЕРДОТЕЛЬНЫХ НАКОПИТЕЛЕЙ
Архипцев Евгений Дмитриевич 68

ОГРАНИЧЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СРЕДСТВ ИСПРАВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ВО ВРЕМЯ ЕГО ВЫПОЛНЕНИЯ
Валеев Денис Рашидович, Котенко Игорь Витальевич 69

РАЗРАБОТКА СТЕНДА ДЛЯ ДИНАМИЧЕСКОГО АНАЛИЗА ЭКСПЛОЙТОВ
Веревкин Сергей Александрович, Федорченко Елена Владимировна 70

ПОСТРОЕНИЕ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ ФЕДЕРАТИВНОГО ОБУЧЕНИЯ
Голубев Сергей Александрович, Новикова Евгения Сергеевна 71

ОБЗОР И СИСТЕМАТИЗАЦИЯ АКТУАЛЬНЫХ МЕТОДОВ РЕАЛИЗАЦИИ ФИШИНГОВЫХ АТАК
Горда Максим Дмитриевич, Чечулин Андрей Алексеевич 72

КОМПЛЕКСНЫЙ ПОДХОД К БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ВКЛЮЧАЯ ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ
Грачев Михаил Иванович, Грачева Наталья Геннадьевна 74

АНАЛИЗ УСЛОВИЙ МОДЕЛИРОВАНИЯ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ В ИНДУСТРИАЛЬНЫХ СИСТЕМАХ ОЧИСТКИ ВОДЫ
Десницкий Василий Алексеевич 75

ОБНАРУЖЕНИЕ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ НА ОСНОВЕ ГРАФО-ОРИЕНТИРОВАННОГО МОДЕЛИРОВАНИЯ СОСТОЯНИЙ СИСТЕМЫ
Десницкий Василий Алексеевич 76

РЕПУТАЦИОННО-ДОВЕРИТЕЛЬНЫЕ МОДЕЛИ ДЛЯ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ НА ОСНОВЕ БЛОКЧЕЙНА
Донсков Евгений Андреевич, Котенко Игорь Витальевич 77

БЕЗОПАСНАЯ ТЕХНОЛОГИЯ ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ
Дубенецкий Владислав Алексеевич, Кузнецов Александр Григорьевич,
Цехановский Владислав Владимирович 78

МОДЕЛЬ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ ДЛЯ ВИЗУАЛЬНОГО АНАЛИЗА ДАННЫХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Жернова Ксения Николаевна 79

ПРОБЛЕМЫ ВИЗУАЛЬНОГО АНАЛИЗА ДАННЫХ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ
Жернова Ксения Николаевна 81

АНАЛИЗ МЕТОДОВ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ,
ПРИМЕНЯЕМЫХ ДЛЯ ОБНАРУЖЕНИЯ МНОГОШАГОВЫХ КИБЕРАТАК
Зеличенок Игорь Юрьевич, Котенко Игорь Витальевич 82

РОЛЬ СТАТИЧЕСКОГО АНАЛИЗАТОРА КОДА
В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОГРАММНОГО ПРОДУКТА
Знаменская Дарья Денисовна 84

О РАЗРАБОТКЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ
УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ
Иванцов Дмитрий Сергеевич, Саенко Игорь Борисович 85

МОДЕЛИ АТАК НА КОМПОНЕНТЫ МАШИННОГО ОБУЧЕНИЯ
СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ КРИТИЧЕСКИХ ИНФРАСТРУКТУР
Ичетовкин Егор Андреевич, Котенко Игорь Витальевич 87

УРОВНИ АРХИТЕКТУРЫ КОМПОНЕНТОВ ОПЕРАТИВНОЙ ОЦЕНКИ
ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ РЕСУРСОВ КРИТИЧЕСКОЙ
ИНФРАСТРУКТУРЫ
Котенко Игорь Витальевич, Саенко Игорь Борисович, Паращук Игорь Борисович 88

АВТОМАТИЗАЦИЯ ПРОЦЕССА ПОДГОТОВКИ МАТЕРИАЛОВ
В РАМКАХ ПРОЕКТА «ПУШКИН ЦИФРОВОЙ»
Котов Александр Александрович, Кокорин Павел Петрович 90

СПОСОБЫ АУТЕНТИФИКАЦИИ И ИХ РОЛЬ В ЗАЩИТЕ ИНФОРМАЦИИ
Крестьяшин Никита Антонович, Пучков Владимир Викторович 91

ОБЗОР АЛГОРИТМОВ ЦИФРОВОЙ ПОДПИСИ СО СКРЫТОЙ ГРУППОЙ
Курышева Алена Андреевна 92

КОНСТРУИРОВАНИЕ ПРИЗНАКОВ АТАК САМООРГАНИЗУЮЩЕЙСЯ ДЕЦЕНТРАЛИЗОВАННОЙ
БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ
Мелешко Алексей Викторович 93

ПОДХОД К РОЛЕВОМУ ФУНКЦИОНИРОВАНИЮ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ
Мелешко Алексей Викторович 95

ОБНАРУЖЕНИЕ АНОМАЛЬНОГО ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ И СУЩНОСТЕЙ
В КОНТЕЙНЕРНЫХ СИСТЕМАХ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ
Мельник Максим Владимирович, Котенко Игорь Витальевич 97

ПОСТРОЕНИЕ СПАМ-ФИЛЬТРА СРЕДСТВАМИ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ
Мокрецов Никита Сергеевич 98

МЕТОД ОБНАРУЖЕНИЯ АНОМАЛЬНОЙ АКТИВНОСТИ И НАРУШЕНИЙ КРИТЕРИЕВ И ПОЛИТИК
БЕЗОПАСНОСТИ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ
Новикова Евгения Сергеевна, Кузнецов Михаил Дмитриевич 100

КОНСИСТЕНТНАЯ БЕЗОПАСНОСТЬ СИСТЕМ УПРАВЛЕНИЯ БОЛЬШИМИ ДАННЫМИ
Полтавцева Мария Анатольевна, Калинин Максим Олегович, Зегжда Дмитрий Петрович 102

СБОР ДАННЫХ ЦИФРОВОЙ КРИМИНАЛИСТИКИ ДЛЯ ЦЕЛЕЙ THREAT HUNTING
Попков Илья Александрович, Котенко Игорь Витальевич[2] 103

СИСТЕМАТИЗАЦИЯ И ОБОБЩЕНИЕ СОБЫТИЙ БЕЗОПАСНОСТИ
Пучков Владимир Викторович, Едемская Екатерина Дмитриевна 104

СНИЖЕНИЕ УЯЗВИМОСТИ СРЕДСТВ ПРОГРАММИРОВАНИЯ
В РАЗЛИЧНЫХ СИСТЕМНЫХ СРЕДАХ ИНФОРМАЦИОННЫХ СИСТЕМ
Соничев Александр Викторович, Щиголева Марина Андреевна, Виноградов Алексей Борисович 105

БЛОЧНОЕ ШИФРОВАНИЕ С ГЕНЕРАТОРОМ СЛУЧАЙНЫХ ЧИСЕЛ
КАК ОСНОВА ДЛЯ ПСЕВДОВЕРОЯТНОСТНОГО ШИФРОВАНИЯ
Татчина Яна Александровна, Уваров Кирилл Андреевич 107

РАЗРАБОТКА КИБЕРФИЗИЧЕСКОГО СТЕНДА ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ ПРОМЫШЛЕННЫХ СИСТЕМ ОЧИСТКИ ВОДЫ
Федорченко Елена Владимировна, Новикова Евгения Сергеевна, Данилов Александр Сергеевич 108

РАССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ КАК ОСНОВА ОПЕРАТИВНОГО АНАЛИЗА КИБЕРБЕЗОПАСНОСТИ И ИСТОЧНИК ИСХОДНЫХ ДАННЫХ ДЛЯ АРХИТЕКТУРНЫХ КОМПОНЕНТОВ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Федорченко Елена Владимировна, Чечулин Андрей Алексеевич, Паращук Игорь Борисович 110

ПРИМЕНЕНИЕ ДИНАМИЧЕСКОЙ ЧЕТЫРЕХЭТАПНОЙ МОДЕЛИ ЗАЩИТЫ ДАННЫХ, ОСНОВАННОЙ НА КРИПТОГРАФИИ И СТЕНОГРАФИИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ
Хлебоказов Виталий Алексеевич, Кушнир Дмитрий Викторович 112

ПОДХОД К ФОРМИРОВАНИЮ ПРИЗНАКОВ ЦЕЛЕВОЙ КИБЕРАТАКИ
ДЛЯ АТРИБУЦИИ КИБЕРНАРУШИТЕЛЯ
Хмыров Семен Сергеевич, Котенко Игорь Витальевич 112

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ 115

АНАЛИЗ ПРОБЛЕМЫ ОБРАБОТКИ ДАННЫХ БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ
Авраменко Владимир Семенович, Чичков Евгений Сергеевич 115

УЯЗВИМОСТИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ
Апарина Елена Юрьевна, Ащеулов Сергей Викторович,
Бабич Борис Иванович, Майер Софья Александровна 117

ЗАЩИТА СЕТЕВЫХ УСТРОЙСТВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА
Апарина Елена Юрьевна, Ащеулов Сергей Викторович,
Бабич Борис Иванович, Патов Григорий Владиславович 119

ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ
ОБРАБОТКИ ИНФОРМАЦИИ
Ащеулов Сергей Викторович, Михайличенко Николай Валерьевич,
Грибков Владимир Александрович, Мишутин Никита Вячеславович 123

ИМИТАЦИОННАЯ МОДЕЛЬ МНОГОКАНАЛЬНОЙ ЭФИРНОЙ СРЕДЫ ПЕРЕДАЧИ ДАННЫХ
Верзун Наталья Аркадьевна, Колбанев Михаил Олегович, Романова Анна Александровна 125

МОНИТОРИНГ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЯ
НА ОСНОВЕ ТЕХНОЛОГИИ ИНТЕРНЕТА ВЕЩЕЙ
Воробьев Андрей Игоревич, Андреева Екатерина Александровна 126

ИССЛЕДОВАНИЕ РЕШЕНИЙ, ОБЕСПЕЧИВАЮЩИХ БЕЗОПАСНОСТЬ
ИНФОРМАЦИОННЫХ РЕСУРСОВ НА ОСНОВЕ ВИРТУАЛЬНЫХ СЕТЕЙ
Горбунов Константин Сергеевич, Пантюхин Олег Игоревич, Солодухин Борис Владимирович 127

К ВОПРОСУ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕТИ
Ильина Ольга Борисовна, Купчиненко Ольга Павловна, Скоропад Александр Витальевич 129

УПРАВЛЕНИЕ ПРОГРАММНЫМИ ПАКЕТАМИ
В СОВРЕМЕННой ОПЕРАЦИОННой СИСТЕМе СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
Ильина Ольга Борисовна, Купчиненко Ольга Павловна, Скоропад Александр Витальевич 131

МЕТОДИКА УПРАВЛЕНИЯ МАРШРУТИЗАЦИЕЙ В СЕТИ ПЕРЕДАЧИ ДАННЫХ
ГРУППЫ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ
Кичко Яна Викторовна, Сапунова Лидия Петровна 133

ПОКАЗАТЕЛИ КАЧЕСТВА И БЕЗОПАСНОСТИ КОНТЕНТА
ЭЛЕКТРОННЫХ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ
В ИНТЕРЕСАХ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ИНЖЕНЕРНОГО ПРОФИЛЯ
Крюкова Елена Сергеевна, Паращук Игорь Борисович 135

О ПРАВАХ ПОЛЬЗОВАТЕЛЯ В ОПЕРАЦИОННОЙ СИСТЕМЕ
Купчиненко Ольга Павловна, Ильина Ольга Борисовна, Скоропад Александр Витальевич 137

РЕАЛИЗАЦИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ СЕТИ ПЕРЕДАЧИ ДАННЫХ
НА ОСНОВЕ ПРОГНОЗИРОВАНИЯ ДЕЙСТВИЙ НАРУШИТЕЛЯ
Липатников Валерий Алексеевич, Шевченко Александр Александрович,
Мелехов Кирилл Витальевич 139

АНАЛИЗ ПРИЧИН ИСКАЖЕНИЯ ДИАГРАММЫ
НАПРАВЛЕННОСТИ БОРТОВЫХ ШИРОКОПОЛОСНЫХ АНТЕНН
Лянгузов Данила Андреевич 141

ИСПОЛЬЗОВАНИЕ МАРШРУТИЗАТОРОВ MIKROTIK
ПРИ ПОСТРОЕНИИ ЗАЩИЩЕННЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ
Мандрик Дмитрий Владимирович, Сазонов Виктор Викторович 141

КРИТЕРИИ ВЫБОРА ЭНЕРГОСБЕРЕГАЮЩЕГО МАРШРУТА
ПЕРЕДАЧИ ДЛЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ С ВЫСОКОЙ ПЛОТНОСТЬЮ
Маслова Дарья Александровна 143

АНАЛИЗ СПОСОБОВ СОЗДАНИЯ ПОГЛОЩАЮЩИХ ГРАНИЧНЫХ УСЛОВИЙ
В МЕТОДЕ КОНЕЧНЫХ РАЗНОСТЕЙ ВО ВРЕМЕННОЙ ОБЛАСТИ
Мешалкин Валентин Андреевич, Шанин Александр Михайлович,
Коньков Денис Иванович, Ткачев Дмитрий Федорович 144

МЕТОДЫ МАРШРУТИЗАЦИИ ОДНОРАНГОВЫХ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ
Миклуш Виктория Александровна 145

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ТЕХНИЧЕСКАЯ НАДЕЖНОСТЬ
МОБИЛЬНЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ: ПОДХОД К ФОРМИРОВАНИЮ ПОКАЗАТЕЛЕЙ ДЛЯ
ТЕКУЩЕГО И ПРОАКТИВНОГО КОНТРОЛЯ
Михайличенко Антон Валерьевич, Паращук Игорь Борисович, Селезнев Андрей Васильевич 146

АНАЛИЗ ПРИМЕНЕНИЯ ЭЛЕМЕНТОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
В ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ТЕХНИЧЕСКОГО ВУЗА
Мнацаканян Владислав Анатольевич, Новосёлов Сергей Витальевич, Пантюхин Олег Игоревич 148

ПОДХОД К ПОСТРОЕНИЮ МОДЕЛИ СЛОЖНОЙ ТЕХНИЧЕСКОЙ СИСТЕМЫ
Остроумов Олег Александрович, Лепешкин Олег Михайлович,
Синюк Александр Демьянович, Ренсков Дмитрий Андреевич 150

ПРОФИЛЬ ФУНКЦИОНИРОВАНИЯ СЛОЖНОЙ ТЕХНИЧЕСКОЙ СИСТЕМЫ
Перов Роман Александрович, Остроумов Олег Александрович, Филимонов Василий Александрович 151

К ВОПРОСУ ИСПОЛЬЗОВАНИЯ ПРОТОКОЛОВ ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ
В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
Рубцова Марина Андреевна, Сазонов Виктор Викторович 153

МЕТОД ОБНАРУЖЕНИЯ АНОМАЛИЙ В SQL-ЗАПРОСАХ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ
Рюмина Светлана Алексеевна, Саенко Игорь Борисович 154

БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ
И БЕЗОПАСНОСТЬ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ
Рязанцева Полина Сергеевна, Михайличенко Николай Валерьевич,
Грибков Владимир Александрович, Ащеулов Сергей Викторович 155

АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ АВТОМАТИЗАЦИИ ДОКУМЕНТООБОРОТА С УЧЕТОМ АНАЛИЗА РИСКОВ ИХ ЗАЩИЩЕННОСТИ
Саяркин Виталий Андреевич, Паращук Игорь Борисович 157

РАЗВИТИЕ КВАНТОВЫХ ТЕХНОЛОГИЙ И ИХ ВЛИЯНИЕ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ
Сергеев Валерий Юрьевич, Михайличенко Николай Валерьевич, Грибков Владимир Александрович, Мишутин Никита Вячеславович 159

ПРИМЕНЕНИЕ СРЕДСТВ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ В БАЗАХ ДАННЫХ
Скоропад Александр Витальевич, Ильина Ольга Борисовна, Купчиненко Ольга Павловна 161

ПОСТРОЕНИЕ СИСТЕМЫ КОМПЬЮТЕРНОЙ ПОДДЕРЖКИ ПРОВЕДЕНИЯ СПЕЦИАЛЬНЫХ УЧЕНИЙ (ИГР)
Солодухин Борис Владимирович, Пантюхин Олег Игоревич, Ковалёв Игорь Станиславович, Пащенко Василий Владимирович, Рябов Геннадий Анатольевич 163

ПРЕДИКТИВНЫЙ КОНТРОЛЬ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ СЛОЖНОЙ ТЕХНИЧЕСКОЙ СИСТЕМЫ
Тесля Сергей Петрович, Остроумов Олег Александрович, Шинкарев Семен Александрович 166

АНАЛИЗ СПОСОБОВ СНИЖЕНИЯ ВЛИЯНИЯ ПЕРЕГРУЗКИ КАНАЛОВ И ТРАКТОВ НА ПРОИЗВОДИТЕЛЬНОСТЬ СПЕЦИАЛИЗИРОВАННОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ В ХОДЕ ЕЕ ФУНКЦИОНИРОВАНИЯ
Титов Владимир Степанович, Апарина Елена Юрьевна, Бабич Борис Иванович, Ащеулов СергейВикторович 168

ПРИМЕНЕНИЕ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ СЕТЕЙ ДЛЯ СИНХРОНИЗАЦИИ БАЗ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
Удальцов Александр Владимирович, Саенко Игорь Борисович 170

ПОДХОД К ОБНАРУЖЕНИЮ И АВТОМАТИЧЕСКОЙ КЛАССИФИКАЦИИ НЕСАНКЦИОНИРОВАННЫХ ВОЗДЕЙСТВИЙ НА ИНФОРМАЦИОННУЮ ТЕЛЕКОММУНИКАЦИОННУЮ СИСТЕМУ
Усов Николай Александрович, Филимонов Василий Александрович, Остроумов Олег Александрович 171

ОБЩИЙ ПОДХОД К ДЕМОДУЛЯЦИИ СИГНАЛОВ С ЦИФРОВОЙ ФАЗОВОЙ МОДУЛЯЦИЕЙ В СИСТЕМАХ СВЯЗИ ДЕКАМЕТРОВОГО ДИАПАЗОНА
Филимонов Василий Александрович, Усов Николай Александрович, Остроумов Олег Александрович 172

ПРИМЕНЕНИЕ РАСПРЕДЕЛЕННОЙ ВИРТУАЛЬНОЙ МАШИНЫ ДЛЯ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ СЕНСОРНОЙ СЕТИ
Шальнев Илья Олегович 174

ЗАДАЧИ СИНТЕЗА ТОПОЛОГИЧЕСКОЙ СТРУКТУРЫ СЕТИ ПЕРЕДАЧИ ДАННЫХ С УЧЕТОМ ПАРАМЕТРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Шинкарев Семен Александрович, Паращук Игорь Борисович 175

ПРИМЕНЕНИЕ МЕТОДА ЭКСТРЕМАЛЬНЫХ ПОРЯДКОВЫХ СТАТИСТИК ДЛЯ ОЦЕНКИ МАЛЫХ ЗНАЧЕНИЙ ВЕРОЯТНОСТЕЙ СЛУЧАЙНЫХ ВЕЛИЧИН
Янковский Никита Андреевич 177

ВЗАИМОСВЯЗЬ МАШИННОГО ЗРЕНИЯ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Яровой Роберт Владимирович, Паращук Игорь Борисович 178

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ 181

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТИ КОМПАНИЙ ПО СОЗДАНИЮ КОМПЬЮТЕРНЫХ ИГР
Аминов Хакимджон Иномджонович, Урванцев Роман Алексеевич 181

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ
СИСТЕМ ВОДОСНАБЖЕНИЯ И ВОДООТВЕДЕНИЯ
Аникин Юрий Викторович, Шилков Владимир Ильич, Ушакова Людмила Ивановна 183

УЛУЧШЕНИЕ МЕТОДОВ ЗАЩИТЫ В СИСТЕМАХ РАДИОЧАСТОТНОЙ АВТОРИЗАЦИИ
Емельянов Александр Александрович, Мелихова Валентина Евгеньевна 185

ПРИОРИТЕТНАЯ МОДЕЛЬ ПРОЦЕССА ОБМЕНА ДАННЫМИ В ЦИФРОВОМ ДВОЙНИКЕ
Краснова Анна Сергеевна, Колбанёв Михаил Олегович 186

ЦИФРОВОЕ СЕЛЬСКОЕ ХОЗЯЙСТВО: НОВЫЕ ТЕХНОЛОГИИ
ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ И БЕЗОПАСНОСТИ В СЕЛЬСКОМ ХОЗЯЙСТВЕ
Маслов Никита Сергеевич 187

О РОЛИ ФЕНОМЕНА АСИММЕТРИИ ВНУТРЕННЕГО ВРЕМЕНИ
В ТЕОРИИ ДОЛГОВЕЧНОСТИ СЛОЖНЫХ ДИНАМИЧЕСКИХ СИСТЕМ
Острейковский Владислав Алексеевич, Сорочкин Андрей Викторович 189

ПРИМЕНЕНИЕ МЕТОДА ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ
ДЛЯ РЕШЕНИЯ ЗАДАЧ СЕТЕВОГО ПЛАНИРОВАНИЯ
Пуха Геннадий Пантелеевич 190

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ИНФРАСТРУКТУРЫ УПРАВЛЕНИЯ
ПРЕДПРИЯТИЕМ С УЧЕТОМ БЕЗОПАСНОСТИ
Соколов Роман Владимирович 192

АНАЛОГИИ ПРЕДСТАВЛЕНИЯ ДАННЫХ. СРАВНЕНИЕ ВЕРБАЛЬНЫХ ВЕЛИЧИН:
ЭКОНОМИКА, ПЛАНОВАЯ ЭКОНОМИКА, РЫНОЧНАЯ ЭКОНОМИКА
Ярошевич Людмила Ивановна 193

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТРАНСПОРТНЫХ СИСТЕМ 194

ПРИМЕНЕНИЕ ERP- И MES-СИСТЕМ В СУДОСТРОИТЕЛЬНОЙ ОТРАСЛИ
Антонова Алёна Евгеньевна, Соколов Сергей Сергеевич 194

МОДЕЛИРОВАНИЕ БЕЗОПАСНЫХТРАНСПОРТНЫХ СИСТЕМ УПРАВЛЕНИЯ
Голоскоков Константин Петрович, Астапкович Алексей Александрович, Коротков Виталий Валерьевич 195

ОПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЕЙ ДВИЖЕНИЯ АВТОНОМНОГО СУДНА ПРИ ПОМОЩИ
ПРОГРАММНОГО ПАКЕТА MAPLE 12
Данилин Герман Владиславович, Соколов Сергей Сергеевич 196

БЕЗОПАСНАЯ СИСТЕМА МОНИТОРИНГА РАЗЛИВОВ НЕФТИ С ИСПОЛЬЗОВАНИЕМ БЕСПИЛОТНЫХ
ЛЕТАТЕЛЬНЫХ АППАРАТОВ
Егорова Кристина Вадимовна, Соколов Сергей Сергеевич 197

МОДЕЛИ ПРОЦЕССА ОБРАБОТКИ ИНФОРМАЦИИ
Зубанова Анастасия Александровна, Когтев Алексей Валерьевич 198

СОЗДАНИЕ БЕЗОПАСНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ТРАНСПОРТНОЙ ЛОГИСТИКИ
НА ОСНОВЕ МУЛЬТИАГЕНТНОГО ПОДХОДА
Искандеров Юрий Марсович 199

ПОДСИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ
ПЕРЕВОЗКИ НЕГАБАРИТНЫХ ГРУЗОВ
Искандеров Юрий Марсович, Чумак Александр Сергеевич, Шахнов Сергей Федорович 201

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ
В РАЗВИТИИ АЛГОРИТМИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРОГНОЗИРОВАНИЯ АСУ
Капустин Артем Сергеевич 202

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ ТРАНСПОРТНЫХ СИСТЕМ
Клионский Дмитрий Михайлович 204

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ВОДНОМ ТРАНСПОРТЕ
Котов Александр Дмитриевич 205

МЕХАНИЗМ ОБЕСПЕЧЕНИЯ ПОЛНОЙ РАНДОМИЗАЦИИ ЦИФРОВОЙ ПОДПИСИ В АЛГЕБРАИЧЕСКИХ АЛГОРИТМАХ СО СКРЫТОЙ ГРУППОЙ
Молдовян Александр Андреевич, Морозова Елена Владимировна 206

ПРИМЕНЕНИЕ ВЕКТОРНЫХ КОНЕЧНЫХ ПОЛЕЙ ПРИ ПОСТРОЕНИИ АЛГОРИТМОВ МНОГОМЕРОЙ КРИПТОГРАФИИ
Морозова Елена Владимировна, Молдовян Николай Андреевич, Костина Анна Александровна 208

О ПРИМЕНЕНИИ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМАХ ЗАЩИТЫ ТРАНСПОРТНЫХ СЕТЕЙ ОТ КИБЕРАТАК
Ныркoв Андрей Анатольевич, Богданова Полина Вадимовна, Прокопенко Даниил Николаевич 210

МЕТОДЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫХ СЕТЯХ ТРАНСПОРТНОЙ ОТРАСЛИ
Ныркoв Анатолий Павлович, Юмашева Елена Сергеевна, Ныркoв Андрей Анатольевич 212

ПРОГРАММНЫЙ КОМПЛЕКС ГЕНЕРАЦИИ БЕЗОПАСНЫХ ПАРОЛЕЙ
Скобелев Алексей Вячеславович, Голоскоков Константин Петрович 213

ДИАЛОГОВЫЕ МОДУЛИ «АИС ИТ КЛИНИКА»
Шипунов Илья Сергеевич, Ныркoв Анатолий Павлович,
Ротнов Дмитрий Александрович, Шипунова Диана Алексеевна 214

О ЗАЩИЩЕННОСТИ КОММУНИКАЦИОННЫХ МОДУЛЕЙ «АИС ИТ КЛИНИКА»
Шипунов Илья Сергеевич, Ныркoв Анатолий Павлович, Шипунова Диана Алексеевна 216

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ 218

IS-АСПЕКТ ИНФОРМАЦИОННО-ПОИСКОВЫХ СИСТЕМ
Азикова Анна Евгеньевна, Озерова Ксения Викторовна, Данильчик Андрей Александрович 218

МЕТОДОЛОГИЯ СОЗДАНИЯ И УЧЕБНО-ЛАБОРАТОРНОГО ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ДВОЙНИКОВ СИСТЕМ АВТОМАТИЗАЦИИ СУДОВ И АУДИТА ИХ ИНФОРМАЦИОННОЙ ЗАЩИЩЕННОСТИ
Алексеев Анатолий Владимирович, Согонов Сергей Александрович,
Максимова Марина Александровна, Хруцкий Олег Валентинович,
Равин Александр Александрович, Михальчук Андрей Васильевич 220

ЦИФРОВИЗАЦИЯ САМОКОНТРОЛЯ ОСВОЕНИЯ ТЕХНОЛОГИЙ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА ПРИ ОПЕРЕЖАЮЩЕМ ОБУЧЕНИИ
Алексеев Анатолий Владимирович, Михальчук Андрей Васильевич, Мусатенко Роман Иванович 222

ИНФОРМАЦИОННАЯ ЖИВУЧЕСТЬ УПРАВЛЕНИЯ: ТЕОРИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОГО ПРЕВОСХОДСТВА
Алексеев Анатолий Владимирович 224

ЦИФРОВОЙ ДВОЙНИК СИСТЕМ АВТОМАТИЗАЦИИ ПРОЦЕССОВ БОРЬБЫ ЗА ИНФОРМАЦИОННУЮ ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА
Алексеев Анатолий Владимирович, Антипов Василий Васильевич, Смольников Александр Васильевич 226

КОНТРОЛЬ ЗА ПРОЯВЛЕНИЕМ ДЕПРЕССИВНОГО СОСТОЯНИЯ У СПЕЦИАЛИСТОВ МОРСКОГО И РЕЧНОГО ФЛОТА, КАК НАПРАВЛЕНИЕ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ СУДОВОЖДЕНИЯ
Артемов Станислав Игоревич, Алексеев Сергей Алексеевич, Рябков Яков Игоревич 228

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИНФОРМАЦИОННОЙ ЖИВУЧЕСТИ
ПРОГРАММНЫХ СИСТЕМ КЛАССА «EAM»
Бондаренко Андрей Игоревич, Головизнина Ольга Игоревна, Алексеев Анатолий Владимирович 230

ОЦЕНКА ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА «MRP»
В ЖИЗНЕННОМ ЦИКЛЕ ОБЪЕКТА МОРСКОЙ ТЕХНИКИ И ИХ ПРИМЕНЕНИЕ
Головизнина Ольга Игоревна, Родоманова Кристина Сергеевна, Алексеев Анатолий Владимирович 232

КВАЛИМЕТРИЧЕСКОЕ РАНЖИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА
«WMS» В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ И ИХ ПРАКТИЧЕСКОЕ ОСВОЕНИЕ
Головизнина Ольга Игоревна, Родоманова Кристина Сергеевна,
Бондаренко Андрей Игоревич, Алексеев Анатолий Владимирович 233

ЦИФРОВОЙ ДВОЙНИК ПРОГРАММНЫХ СРЕДСТВ РЕАЛИЗАЦИИ
СЕРВИСА CRM В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ
Егоров Ахмед Сахибович, Дуркин Илья Константинович,
Никоноров Владислав Юрьевич, Едошин Александр Дмитриевич 235

КВАЛИМЕТРИЧЕСКОЕ РАНЖИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА «PDM» В ЖЦ
ОМИ ТИПА АО ЦМКБ «АЛМАЗ» И ИХ ПРАКТИЧЕСКОЕ ОСВОЕНИЕ
Парастаева Елена Игоревна, Калинина Алена Михайловна,
Тюрина Наталья Анатольевна, Алексеев Анатолий Владимирович 237

ЗАДАЧА ПОИСКА ОПТИМАЛЬНОГО ПОЛОЖЕНИЯ ЦЕНТРА УПРАВЛЕНИЯ В БЕЗОПАСНОМ
ИСПОЛНЕНИИ В ВЫСОТНОМ ЗДАНИИ МОРСКОЙ ИНФРАСТРУКТУРЫ
Плотников Павел Владимирович, Алексеев Сергей Алексеевич 239

ПРИНЦИПЫ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ НАУЧНО-
ПРОИЗВОДСТВЕННЫХ ОБЪЕДИНЕНИЙ МОРСКОЙ ИНФРАСТРУКТУРЫ
Рябков Яков Игоревич, Алексеев Сергей Алексеевич, Артемов Станислав Игоревич 241

ФОРМИРОВАНИЕ СПИСКА РЕКОМЕНДАЦИЙ
ДЛЯ МОДЕРНИЗАЦИИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПО РЕЗУЛЬТАТАМ ОЦЕНКИ УРОВНЯ ЗРЕЛОСТИ ПРЕДПРИЯТИЯ
Тарасов Валентин Сергеевич, Кудинова Екатерина Андреевна 243

РАНЖИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
КЛАССА «FM» В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ
Юрков Антон Николаевич 244

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ 247

СИГНИФИКАТИВНО-ДЕНОТАТИВНЫЙ ПЕРЕНОС
В ТЕХНОЛОГИИ МАНИПУЛЯЦИИ СОЗНАНИЕМ
Беломестнова Нина Васильевна 247

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННО-ПОЛИТИЧЕСКОМУ ВОЗДЕЙСТВИЮ
НА ДОЛЖНОСТНОЕ ЛИЦО
Борщенко Виктор Владимирович 248

СОЦИОКУЛЬТУРНАЯ ТРАНСФОРМАЦИЯ УКРАИНСКОГО ОБЩЕСТВА: АЛЬТЕРНАТИВНЫЕ
КОНЦЕПЦИИ В КОНТЕКСТЕ ЭВОЛЮЦИОННЫХ И ЦИКЛИЧНЫХ ТЕОРИЙ
Дегтярева Ольга Викторовна 251

ТЕХНОЛОГИИ КОГНИТИВНОЙ БЕЗОПАСНОСТИ НА ПУТИ ИНТЕГРАЦИИ
Кефели Игорь Федорович 252

ПРАВОВЫЕ ОСНОВЫ КОГНИТИВНОЙ БЕЗОПАСНОСТИ
Кириленко Виктор Петрович, Алексеев Георгий Валерьевич 254

МЕДИАОБРАЗ СОВРЕМЕННОЙ РОССИИ В СМИ ГРЕЦИИ
Кучинская Яна Францевна 256

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В МЕДИЙНОЙ СФЕРЕ:
ПРОГРЕСС ИЛИ УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?
Лай Линчжи 257

ВЛИЯНИЕ СЕТЕВЫХ МЕДИА НА ФОБИИ И УРОВЕНЬ ПСИХОЛОГИЧЕСКОЙ ТРЕВОЖНОСТИ
В АСПЕКТЕ КОГНИТИВНОЙ БЕЗОПАСНОСТИ
Мельник Вероника Родионовна 258

МЕДИЙНЫЕ РЕСУРСЫ В ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ АТАКАХ
НА РОССИЙСКУЮ ГОСУДАРСТВЕННОСТЬ
Мельник Галина Сергеевна 260

МАССМЕДИА ГЕРМАНИИ КАК СРЕДСТВО КОГНИТИВНОГО ИСКАЖЕНИЯ РЕАЛЬНОСТИ
Мисонжников Борис Яковлевич 261

К ВОПРОСУ О ПОНЯТИИ КОГНИТИВНОГО ПРОСТРАНСТВА
Плебанек Ольга Васильевна 264

ТЕОРИЯ ФРЕЙМИНГА И ПОЛИТИЗАЦИЯ СМИ (НА ПРИМЕРЕ ЗАМАЛЧИВАНИЯ
ЗАПАДНЫМИ МЕДИА ПРОБЛЕМЫ СБРОСА ЯПОНИЕЙ ЯДЕРНЫХ ОТХОДОВ В МОРЕ)
Тань Лэи 265

МЕДИАПОТРЕБЛЕНИЕ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ:
НЕГАТИВНЫЕ И ПОЗИТИВНЫЕ ПОСЛЕДСТВИЯ
Тюнина Екатерина Владимировна 268

ИССЛЕДОВАНИЕ ПОВЕДЕНИЯ И ПСИХОЛОГИИ ВЕРБАЛЬНОГО НАСИЛИЯ
СРЕДИ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ-СМИ
Чжоу Шэннань 269

НЕЙРОНАУКИ – ОСНОВА ИССЛЕДОВАНИЯ ОСОБЕННОСТЕЙ ГОЛОВНОГО МОЗГА И
МОДЕЛИРОВАНИЯ РАЗЛИЧНЫХ КОГНИТИВНО-ПОВЕДЕНЧЕСКИХ ПРОЦЕССОВ
Шангин Андрей Борисович 271

ОСНОВНЫЕ НАПРАВЛЕНИЯ ИНФОРМАЦИОННОГО-ПОДРЫВНОЙ ДЕЯТЕЛЬНОСТИ ЗАПАДА ПРОТИВ
РОССИЦЙСКОЙ ФЕДЕРАЦИИ: ПОЛИТОЛОГИЧЕСКИЙ АНАЛИЗ
Шевцов Владимир Сергеевич 273

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ 276

СПОСОБ УСКОРЕНИЯ ПРОВЕДЕНИЯ ГЛОБАЛЬНОГО АПОСТЕРИОРНОГО ВЫВОДА
С ИСПОЛЬЗОВАНИЕМ ТРЕТИЧНОЙ СТРУКТУРЫ
Абрамов Максим Викторович, Вяткин Артём Андреевич 276

ВЛИЯНИЕ СОЦИОИНЖЕНЕРНЫХ АТАК НА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И
ФУНКЦИОНИРОВАНИЕ РЕГИОНАЛЬНЫХ ГОСУДАСРТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
Азаров Артур Александрович, Демидов Михаил Олегович, Савельев Павел Сергеевич 277

СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ ФАКТОРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И
ФУНКЦИОНИРОВАНИЯ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В КОНТЕКСТЕ
СОЦИОИНЖЕНЕРНЫХ АТАК
Азаров Артур Александрович, Демидов Михаил Олегович, Савельев Павел Сергеевич 278

ЦИФРОВОЕ РАБСТВО КАК УГРОЗА ЦИФРОВОЙ ТРАНСФОРМАЦИИ
ЛИЧНОСТИ ОТ ПРАВОВЫХ ИНСАЙДЕРОВ
Алексеев Анатолий Владимирович 279

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В БОРЬБЕ С НЕСАНКЦИОНИРОВАННЫМ ДОСТУПОМ:
ЗАЩИТА ОТ АТАК, ИСПОЛЬЗУЮЩИХ МЕССЕНДЖЕРЫ СЕТИ ИНТЕРНЕТ
Бобрышов Данил Павлович, Зацепин Илья Сергеевич, Чуваев Константин Игоревич 281

ЗАДАЧА РАЗРАБОТКИ СЕРВИСА ПЛАНИРОВАНИЯ СТОИМОСТИ АВТОМОБИЛЬНОГО МАРШРУТА С УЧЁТОМ ПОЛЬЗОВАТЕЛЬСКИХ ПАРАМЕТРОВ
Корепанова Анастасия Андреевна, Есин Максим Сергеевич, Сабреков Артём Азатович 282

СИСТЕМА АВТОМАТИЗИРОВАННОГО КОНТРОЛЯ СТАБИЛЬНОСТИ ФУНКЦИОНИРОВАНИЯ СЕРВИСА РАСЧЕТА СТОИМОСТИ ДОСТАВКИ НА ЛОГИСТИЧЕСКОМ ПОРТАЛЕ CARGOTIME.RU
Назарова Полина Андреевна, Есин Максим Сергеевич, Сабреков Артём Азатович 283

ОЦЕНКА СКЛОННОСТИ КОМПОНЕНТОВ ТЕХНИЧЕСКОЙ СИСТЕМЫ К ОТКАЗАМ С УЧЕТОМ ВНЕШНИХ И ВНУТРЕННИХ ФАКТОРОВ ПО ОГРАНИЧЕННЫМ ДАННЫМ ОБ ОШИБКАХ
Столярова Валерия Фуатовна, Тулупьев Александр Львович 285

РАЗРАБОТКА МЕТОДА ВЫЯВЛЕНИЯ ФЕЙКОВЫХ АККАУНТОВ В СОЦИАЛЬНЫХ СЕТЯХ
Низомутдинов Борис Абдуллохонович 286

КОГНИТИВНОЕ МОДЕЛИРОВАНИЕ ВЗРЫВООБРАЗНОГО РАСПРОСТРАНЕНИЯ ИНВАЗИВНОЙ ИНФОРМАЦИИ В НЕСТАБИЛЬНОМ СОЦИУМЕ
Переварюха Андрей Юрьевич, Манвелова Александра Борисовна, Трофимова Инна Владимировна
Михайлов Владимир Валентинович, Хасанов Дмитрий Салимович 288

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ 291

ПРИМЕНЕНИЕ МЕТОДОВ КОМПЬЮТЕРНОЙ МАТЕМАТИКИ И КРАТНОМАСШТАБНОГО АНАЛИЗА ДЛЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ИНФОРМАЦИОННЫЕ СИСТЕМЫ
Бортникер Петр Владимирович, Саенко Игорь Борисович 291

ОПИСАНИЕ ТЕХНОЛОГИИ РАСПОЗНАВАНИЯ ОБРАЗОВ
ПРИ ВЫЯВЛЕНИИ ДОРОЖНО-ТРАНСПОРТНЫХ ПРОИСШЕСТВИЙ
Галеева Евгения Алексеевна 292

РАСПОЗНАВАНИЕ ДОРОЖНО-ТРАНСПОРТНЫХ ПРОИСШЕСТВИЙ
С ПОМОЩЬЮ КОМПЬЮТЕРНОГО ЗРЕНИЯ
Головкин Матвей Максимович 293

МЕТОД СИМБИОТИЧЕСКОГО ВЗАИМОДЕЙСТВИЯ НЕЙРОННЫХ СЕТЕЙ
С ОТСУТСТВИЕМ ЭЛЕМЕНТОВ АНТАГОНИСТИЧЕСКОЙ ИГРЫ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ НАБОРОВ ДАННЫХ
Гололобов Никита Вячеславович, Павленко Евгений Юрьевич 294

ВАРИАНТ ПОСТРОЕНИЯ ИЗМЕРИТЕЛЬНОЙ СЕТИ УРОВНЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА КОНТРОЛЛЕРАХ IoT
Кулешов Сергей Викторович, Аксенов Алексей Юрьевич 296

СОЧЕТАНИЕ ПОНЯТИЙ ОТКРЫТОСТИ И БЕЗОПАСНОСТИ
В ПРОТОТИПЕ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ
Нечитайленко Роман Александрович, Глущенко Артём Геннадьевич, Денисов Егор Юрьевич 297

МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ
Пахомов Максим Анатольевич, Соболев Николай Владиславович, Павленко Евгений Юрьевич 299

КЛАСТЕРИЗАЦИЯ ДАННЫХ С ПРИМЕНЕНИЕМ НЕЙРОННОЙ СЕТИ КОХОНЕНА
Швайко Александр Сергеевич 301

ПРИНЦИПЫ ПОСТРОЕНИЯ САМООРГАНИЗУЮЩЕЙСЯ КАРТЫ НЕЙРОСЕТИ
ДЛЯ АРХИТЕКТУРЫ ЗАЩИЩЕННОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ
ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ И ИНЦИДЕНТОВ
Штеренберг Станислав Игоревич 302

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ МАШИННОГО ЗРЕНИЯ
В УСЛОВИЯХ ОГРАНИЧЕННЫХ РЕСУРСОВ
Яковлева Екатерина Арнольдовна 303

ОДИН ИЗ ВАРИАНТОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ НА ЕДИНОЙ ПЛАТФОРМЕ
Янковский Никита Андреевич, Татарникова Татьяна Михайловна 304

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 307

СОВЕРШЕНСТВОВАНИЕ ПЕДАГОГИЧЕСКИХ МЕТОДИК ПОСРЕДСТВОМ ПРИМЕНЕНИЯ ВИРТУАЛЬНОГО ЛАБОРАТОРНОГО ПРАКТИКУМА ПРИ ИЗУЧЕНИИ КУРСАНТАМИ ОСНОВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
Воронов Сергей Алексеевич, Примакин Алексей Иванович 307

ПОДГОТОВКА БУДУЩИХ КАДРОВ ПО УПРАВЛЕНИЮ БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ
Грачев Александр Михайлович 308

БОРЬБА С УГРОЗАМИ В СОЦИАЛЬНЫХ СЕТЯХ
Кононов Олег Александрович, Кононова Ольга Васильевна 309

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ ПРОЦЕССОМ ПРОВЕДЕНИЯ КЛИНИЧЕСКОЙ ПРАКТИКИ СТУДЕНТАМИ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ
Сафронова Мария Вадимовна, Ныркov Анатолий Павлович 311

РАЗРАБОТКА ЦИФРОВОЙ БИРЖИ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ РЕЗУЛЬТАТОВ ПГУПС
Соломатова Мария Феликсовна, Смелов Илья Максимович,
Доцаев Тимур Артурович, Пак Владислав Павлович 313

ИЗУЧЕНИЕ МЕХАНИЗМОВ ИЗОЛЯЦИИ РЕСУРСОВ ОПЕРАЦИОННОЙ СИСТЕМЫ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО «КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»
Частухин Даниил Алексеевич, Широков Владимир Владимирович, Щиголева Марина Андреевна 314

ВИРТУАЛЬНЫЙ ТРЕНАЖЕР КАК СПОСОБ ОБУЧЕНИЯ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ
Шейхов Глеб Вагифович, Липатников Валерий Алексеевич, Островский Юрий Николаевич,
Васильев Никита Алексеевич, Ледовская Кристина Геннадьевна 316

ПРОЕКТ «ИТ КЛИНИКИ» В ГУМРФ ИМЕНИ АДМИРАЛА С. О. МАКАРОВА»
Шипунов Илья Сергеевич, Ныркov Анатолий Павлович, Шипунова Диана Алексеевна 317

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «ЭКОСИСТЕМА БЕЗОПАСНЫХ ГОРОДСКИХ ЦИФРОВЫХ СЕРВИСОВ» 320

ОБЗОР ПОДХОДОВ К ОЦЕНКЕ ЦИФРОВЫХ СЕРВИСОВ
Аркатов Дмитрий Александрович 320

ПРОНИКНОВЕНИЕ ЦИФРОВЫХ МЕДИЦИНСКИХ СЕРВИСОВ В СРЕДУ ПОЖИЛЫХ ЖИТЕЛЕЙ ПЕТЕРБУРГА
Видясова Людмила Александровна, Толстикова Ирина Ивановна 321

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ГОСУДАРСТВЕННЫХ СЕРВИСОВ КАК ФАКТОР СОЦИАЛЬНОГО САМОЧУВСТВИЯ: НА ПРИМЕРЕ САНКТ-ПЕТЕРБУРГА
Видясова Людмила Александровна, Якубова Мария Юрьевна 322

ПРАВО НА ОТКАЗ ОТ ЦИФРОВЫХ ТЕХНОЛОГИЙ В УСЛОВИЯХ ДИНАМИЧНОЙ ЦИФРОВИЗАЦИИ ОБЩЕСТВА
Денисов Денис Сергеевич 324

РАЗРАБОТКА ЦИФРОВЫХ СЕРВИСОВ ПО ОПТИМИЗАЦИИ РАСХОДОВ ГОРОДСКОГО БЮДЖЕТА НА ФИНАНСИРОВАНИЕ ФАРМАКОТЕРАПИИ ДЛЯ ПАЦИЕНТОВ С ОНКОЛОГИЧЕСКИМИ ЗАБОЛЕВАНИЯМИ
Каневский Максим Александрович 326

ВОСПРИЯТИЕ ЦИФРОВЫХ ГОСУДАРСТВЕННЫХ СЕРВИСОВ
ГРАЖДАНСКИМИ АКТИВИСТАМИ САНКТ-ПЕТЕРБУРГА
Киселева Дарья Александровна, Сунгуров Александр Юрьевич 327

АНАЛИЗ ВНЕДРЕНИЯ ЭКОСИСТЕМЫ ГОРОДСКИХ СЕРВИСОВ «ЦИФРОВОЙ ПЕТЕРБУРГ»
Кузнецов Алексей Геннадьевич 329

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ СЕРВИСОВ В МУНИЦИПАЛИТЕТАХ САНКТ-ПЕТЕРБУРГА
Метелева Алина Сергеевна, Слав Юлия Эдуардовна, Филатова Ольга Георгиевна 330

ЭКОСИСТЕМА ГОРОДСКИХ СЕРВИСОВ «ЦИФРОВОЙ ПЕТЕРБУРГ»
Осмоловский Кирилл Евгеньевич 332

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЦИФРОВЫХ СЕРВИСОВ С УЧЕТОМ СПЕЦИФИКИ ДОВЕРИЯ
ПОЖИЛЫХ ПОЛЬЗОВАТЕЛЕЙ К ОНЛАЙН-ПЛАТФОРМАМ
Равчик Михаил Игоревич 333

РАЗРАБОТКА БАЗЫ ДАННЫХ ДЕСТРУКТИВНОГО КОНТЕНТА
НА ОСНОВЕ ДАННЫХ ИЗ МЕССЕНДЖЕРОВ
Углова Анна Борисовна, Низомутдинов Борис Абдуллохонович 335

РОЛЕВАЯ МОДЕЛЬ ЭКОСИСТЕМЫ ГОРОДСКИХ СЕРВИСОВ:
ИССЛЕДОВАНИЕ ПОТРЕБНОСТЕЙ БИЗНЕС-СФЕРЫ
Юпланов Марк Намикович 336

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ» 339

ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ В ЗАДАЧЕ АВТОНОМНОЙ НАВИГАЦИИ БЕСПИЛОТНЫХ
ЛЕТАТЕЛЬНЫХ АППАРАТОВ
Беляев Павел Юрьевич, Зикратов Игорь Алексеевич 339

СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЦИФРОВЫХ ДВОЙНИКОВ
ПРОСТРАНСТВЕННЫХ ОБЪЕКТОВ
Верхова Галина Викторовна, Акимов Сергей Викторович,
Прощенков Валерий Михайлович, Юрчик Даниил Сергеевич 340

ИССЛЕДОВАНИЕ И РАЗРАБОТКА АЛГОРИТМОВ ДИНАМИЧЕСКОЙ СТЕГАНОГРАФИИ
ДЛЯ ГРАФИЧЕСКИХ КОНТЕЙНЕРОВ
Волынкин Павел Александрович, Гибадуллин Альберт Артурович 341

РАЗРАБОТКА МЕТОДИКИ, АЛГОРИТМИЧЕСКОГО И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОЦЕНКИ
КАЧЕСТВА ШИФРОВАНИЯ
Волынкин Павел Александрович, Кузнецов Вадим Всеволодович 342

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ТЕХНОЛОГИИ OWE
В БЕСПРОВОДНОЙ СЕТИ СО СТАНДАРТОМ WPA3
Герлинг Екатерина Юрьевна, Зебзеев Егор Алексеевич, Кистуга Антон Юрьевич 343

ИССЛЕДОВАНИЕ ИНФОРМАЦИОННОЙ МОДЕЛИ ОЦЕНКИ УРОВНЯ ПОДГОТОВКИ СТУДЕНТОВ ПРИ
ТЕСТИРОВАНИИ
Губин Александр Николаевич, Михайлова Екатерина Александровна 344

ОБНАРУЖЕНИЕ АТАКИ НА TDLS БЕСПРОВОДНОГО УСТРОЙСТВА
Дрепа Владислав Евгеньевич, Ковцур Максим Михайлович,
Сахаров Дмитрий Владимирович, Шарапов Роман Игоревич 345

НОВЫЙ ПОДХОД К ИССЛЕДОВАНИЮ ЦЕЛОСТНОСТИ
ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX В ПРОЦЕССЕ ЕЕ РАБОТЫ
Коньков Владимир Владимирович, Кузнецов Владимир Александрович, Красов Андрей Владимирович 346

СРАВНИТЕЛЬНЫЙ АНАЛИЗ БИБЛИОТЕК ДЛЯ РЕШЕНИЯ ЗАДАЧ ОБРАБОТКИ ЕСТЕСТВЕННОГО ЯЗЫКА
Копытова Елена Вячеславовна, Филиппов Феликс Васильевич 348

ВЫБОР МОДУЛЯ ЯДРА ОС LINUX ДЛЯ ВНЕДРЕНИЯ ЦВЗ
Красов Андрей Владимирович 349

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ В НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЯХ
Литвинов Владислав Леонидович, Балакирев Николай Александрович 351

ПРИНЦИПЫ БЕЗОПАСНОГО ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ
Литвинов Владислав Леонидович, Безкоровайная Мария Валерьевна,
Толмачев Андрей Юрьевич, Гольдес Илья Станиславович 353

ИССЛЕДОВАНИЕ МЕТОДОВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ
ПРОЦЕССОВ РАСПРОСТРАНЕНИЯ ЭПИДЕМИИ
Литвинов Владислав Леонидович, Дергачев Даниил Денисович 354

РАЗВИТИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ ВРЕДОНОСНОГО ПРИМЕНЕНИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
Литвинов Владислав Леонидович, Гольдес Илья Станиславович,
Безкоровайная Мария Валерьевна, Толмачев Андрей Юрьевич 355

АНАЛИЗ АТАК НА СЕТЕВЫЕ УЗЛЫ ГРУППОВЫХ РОБОТОВ
Литвинов Владислав Леонидович, Яшин Алексей Владимирович 356

МЕТОД ФОРМИРОВАНИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ
СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ С УЧЕТОМ ИМЕЮЩИХСЯ РЕСУРСОВ
Липатников Валерий Алексеевич, Парфиров Виталий Александрович, Петренко Михаил Игоревич 357

ОБЗОР ИССЛЕДОВАНИЙ ПО ОЦЕНКЕ ПРОИЗВОДИТЕЛЬНОСТИ WLAN СЕТИ
Махмутова Нурия Фаритовна, Ковцур Максим Михайлович,
Петрова Татьяна Васильевна, Киструга Антон Юрьевич 359

ИССЛЕДОВАНИЕ ПРОГРАММНОЙ СТРУКТУРЫ АРХИТЕКТУРЫ СЕТИ РАДИОДОСТУПА LTE
Мошак Николай Николаевич, Кравец Алексей Юрьевич 360

IPX НОВАЯ ПАРАДИГМА КОНВЕРГЕНЦИИ МОБИЛЬНЫХ И ФИКСИРОВАННЫХ СЕТЕЙ NGN
Мошак Николай Николаевич, Медведев Дмитрий Сергеевич 363

АНАЛИЗ РАСПРЕДЕЛЕННОГО ПЛАНИРОВАНИЯ ДЕЙСТВИЙ В МУЛЬТИАГЕНТНЫХ СИСТЕМАХ
Пелих Дмитрий Александрович, Птицына Лариса Константиновна, Ширин Александр Игоревич 364

ИССЛЕДОВАНИЕ ИНСТРУМЕНТАРИЯ WEBSPLOIT ДЛЯ ОЦЕНКИ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ БЕСПРОВОДНОЙ СЕТИ
Петрова Татьяна Васильевна, Кузьмина Ольга Ивановна,Ковцур Максим Михайлович, Киструга Антон Юрьевич ... 365

ОНТОЛОГИЯ АРХИТЕКТУРЫ ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ПРОГНОЗА
БИРЖЕВЫХ КОТИРОВОК
Птицын Никита Алексеевич, Птицына Лариса Константиновна 366

МИКРОСЕРВИСЫ ПОВЫШЕНИЯ КАЧЕСТВА ПОИСКА ИНФОРМАЦИИ
Птицына Лариса Константиновна, Солтык Алексей Михайлович 368

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ НА ОСНОВЕ ИММУНОКОМПЬЮТИНГА
Тюменцев Алексей Андреевич, Бондаренко Игорь Борисович 369

ПРИМЕНЕНИЕ ТЕОРИИ БИФУРКАЦИЙ ДЛЯ АНАЛИЗА КИБЕРБЕЗОПАСНОСТИ
ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ
Шашкин Владислав Сергеевич, Петрова Татьяна Сергеевна, Бирих Эрнест Владимирович,
Сахаров Дмитрий Владимирович, Липатников Валерий Алексеевич 370

ОГЛАВЛЕНИЕ 373

CONTENTS

STATE POLICY OF ENSURING INFORMATION SECURITY OF THE REGIONS OF RUSSIA 16

RISK ASSESSMENT IN REGIONAL MANAGEMENT
Buldakova Tatiana, Dzhalolov Ahmad 16

CYBERSECURITY AND RELATED CONCEPTS. SCIENTIFIC AND METHODOLOGICAL ASPECTS IN THE CONDITIONS OF MODERN INFORMATION WARFARE
Zhigadlo Valentin 17

FREE SOFTWARE AND SECURITY OF STATE INFORMATION SYSTEMS AND CRITICAL INFORMATION INFRASTRUCTURE OBJECTS
Karpov Roman 19

METHODOLOGY AND TECHNOLOGIES FOR PROACTIVE MANAGEMENT AND CONTROL FOR MODERNIZATION OF DISASTER-TOLERANCE INFORMATION SYSTEMS
Okhtilev Mikhail, Sokolov Boris, Yusupov Rafael 21

FUNDAMENTALS OF STATE POLICY ON DETECTING, PREVENTING AND ELIMINATING THE CONSEQUENCES OF COMPUTER ATTACKS ON THE INFORMATION RESOURCES OF THE RUSSIAN FEDERATION AND RESPONDING TO COMPUTER INCIDENTS
Storozhik Viktor 23

DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE INTERESTS OF INDUSTRY IN THE RUSSIAN ARCTIC
Mitko Arseny, Sidorov Vladimir 26

LEGAL ASPECTS OF INFORMATION SECURITY 28

THREATS TO INFORMATION SECURITY IN COMPUTER SYSTEMS. SOURCES OF OCCURRENCE, MEANS AND METHODS OF PROTECTION
Vasyutina Tatiana, Fayzulin Almaz 28

ELECTRONIC COURSE MANAGEMENT SYSTEM IN THE CONTEXT OF DIGITALIZATION OF EDUCATIONAL ACTIVITIES
Voronov Sergey, Primakin Alexey 29

STATE GUARANTEE OF INDIVIDUAL RIGHTS AND FREEDOMS, LEGAL ASPECTS OF NATIONAL SECURITY
Gromova Olga 31

APPLICATION OF FACTOR AND VARIANCE ANALYSIS ALGORITHMS FOR FORMATION AND IDENTIFICATION OF PRIORITY FACTORS DETERMINING LEVEL OF INFORMATION PROTECTION IN POWER UNITS
Efimova Anna, Primakin Alexey 34

APPLICATION OF GAME THEORY TO ENSURE INFORMATION SECURITY IN ROSGVARDIA UNITS
Efimova Anna, Primakin Alexey 35

ON THE NEED FOR ENGINEERING AND TECHNICAL TRAINING OF FUTURE ROSGVARDIA OFFICERS TO SOLVE PROBLEMS OF ENSURING INFORMATION SECURITY IN THE SYSTEM OF PROTECTING NATIONAL INTERESTS OF RUSSIA
Zozulin Igor, Primakin Alexey 36

ENSURING INFORMATION SECURITY AT THE OBJECT OF CRITICAL INFORMATION INFRASTRUCTURE
Loknov Alexey, Simakova Ekaterina 37

INFORMATION SECURITY AUDIT AS A MEASURE OF INFORMATION PROTECTION AT THE ATS INFORMATIZATION FACILITY
Lopatin Bogdan, Yakushev Denis 39

DATA PROTECTION IN THE DIGITAL AGE
Milovanov Andrew, Shalaginova Olga 40

WAYS OF PROTECTION AND MEASURES OF RESPONSIBILITY
FOR VIOLATION OF THE LAW ON PERSONAL DATA
Parfenov Nikolai, Shalaginova Olga, Karpov Pavel 42

FORMATION OF A SYSTEM OF INDICATORS DETERMINING THE DEGREE
OF INFORMATION PROTECTION OF ROSGVARDIA STRUCTURAL UNITS IN CONDITIONS
OF INFORMATION CONFRONTATION
Potapova Ludmila, Primakin Alexey 43

ANALYSIS OF CYBERSECURITY THREATS IN THE FIELD OF HEALTHCARE
Pronsky Alexander Yurievich, Shalaginova Olga Borisovna 44

ASPECTS OF THE USE OF NON-CRIMINALISTIC INFORMATION SYSTEMS
Prourzina Olga 46

INFORMATION SECURITY AUDIT AS A MEASURE OF INFORMATION PROTECTION
AT THE ATS INFORMATIZATION FACILITY
Rogova Yuliya, Yakushev Denis 48

LEGAL JUSTIFICATION OF THE ROLE AND PLACE OF FIRE SAFETY
IN ENSURING INFORMATION SECURITY
Sineshchuk Yury, Terehin Sergey, Shidlovsky Grigory 50

METHODS OF INFORMATION PROTECTION IN THE SYSTEM
OF PREVENTION OF CORRUPTION CRIMES
Sineshchuk Yury, Loknov Aleksey 51

INFORMATIZATION OF LIBRARIES AS A KEY DIRECTION
OF THE STATE LIBRARY POLICY OF RUSSIA
Sakhno Roman 52

INFORMATION AND ANALYTICAL SUPPORT IN MILITARY AFFAIRS
Shalaginova Olga Borisovna 54

MATHEMATICS IN THE FIGHT AGAINST CRIME
Shalaginova Olga 55

LEGAL ASPECTS OF INFORMATION AND PSYCHOLOGICAL WELL-BEING
OF THE INDIVIDUAL IN THE CONTEXT OF DIGITAL TRANSFORMATION
Shilkov Vladimir 57

A METHOD FOR ASSESSING THE LEVEL OF INITIAL SECURITY
OF PERSONAL DATA INFORMATION SYSTEMS
Yakovleva Natalia, Bolshakova Valentina, Sibarov Konstantin, Karpov Pavel 59

TO THE QUESTION OF USING A DISTRIBUTED REGISTRY FOR STORING INFORMATION
IN THE ACTIVITIES OF THE INTERNAL AFFAIRS BODIES OF RUSSIA
Yakushev Denis, Bushmanov Nikita 60

JUSTIFICATION OF THE NEED TO IMPROVE THE METHODS
OF PERSONAL DATA PROTECTION IN DEPARTMENTAL INFORMATION SYSTEMS
Yakushev Denis, Zhaldak Anastasia 62

GROUP SECURITY POLICY AS A WAY TO INCREASE THE SECURITY OF OBJECTS
OF INFORMATIZATION OF INTERNAL AFFAIRS BODIES
Yakushev Denis, Lukina Ksenia 64

SECURITY OF INFORMATION TECHNOLOGY **67**

THE PROBLEM OF SECURITY IN GATHERING, STORING AND USING DATA WHEN WORKING WITH DIGITAL TWINS OF PEOPLE
Ananeva Varvara 67

MODEL OF LIFE DEVELOPMENT OF SOLID-STATE DRIVES
Arkhiptsev Evgeny 68

LIMITATIONS AND OUTLOOK FOR SOFTWARE RUNTIME PATCHING TOOLS
Valeev Denis, Kotenko Igor 69

DEVELOPMENT OF THE TESTBED FOR DYNAMIC ANALYSIS OF EXPLOITS
Verevkin Sergey, Fedorchenko Elena 70

DESIGN OF A DISTRIBUTED INTRUSION DETECTION SYSTEM BASED ON FEDERATED LEARNING
Golubev Sergei, Novikova Evgenia 71

REVIEW AND SYSTEMATIZATION OF RELEVANT PHISHING ATTACKS TECHNIQUES
Gorda Maxim, Chechulin Andrey 72

INTEGRATED APPROACH TO ENTERPRISE SECURITY INCLUDING SIMULATION MODELING
Grachev Mikhail, Gracheva Natalya 74

ANALYSIS OF MODELING CONDITIONS OF ATTACKS IN INDUSTRIAL WATER PURIFICATION SYSTEMS
Desnitsky Vasily 76

DETECTION OF ATTACKS ON GRAPH-BASED MODELING OF SYSTEM STATES
Desnitsky Vasily 77

REPUTATION AND TRUST MODELS FOR INTELLIGENT TRANSPORT SYSTEMS BASED ON BLOCKCHAIN
Donskov Evgenii, Kotenko Igor 78

SAFE DESIGN TECHNOLOGY INFORMATION SYSTEMS
Dubenetsky Vladislav, Kuznetsov Alexander, Tsekhanovsky Vladislav 79

ARTIFICIAL NEURAL NETWORK MODEL FOR VISUAL ANALYSIS OF INFORMATION SECURITY DATA
Zhernova Ksenia 80

PROBLEMS OF VISUAL ANALYSIS OF DATA IN THE FIELD OF INFORMATION SECURITY USING ARTIFICIAL NEURAL NETWORKS
Zhernova Ksenia 81

ANALYSIS OF BIG DATA PROCESSING METHODS USED TO DETECT MULTI-STEP CYBER ATTACKS
Zelichenok Igor, Kotenko Igor 82

THE ROLE OF A STATIC CODE ANALYZER IN INFORMATION SECURITY OF THE PROGRAM PRODUCT
Znamenskaya Daria 84

ON THE DEVELOPMENT OF A MATHEMATICAL MODEL OF THE PROCESS OF OPERATION OF THE INFORMATION AND SECURITY EVENT MANAGEMENT SYSTEM
Dmitry Ivantsov, Igor Saenko 85

MODELS OF ATTACKS ON MACHINE LEARNING COMPONENTS OF INTRUSION DETECTION SYSTEMS FOR CRITICAL INFRASTRUCTURES
Ichetovkin Egor, Kotenko Igor 87

LEVELS OF ARCHITECTURE OF COMPONENTS OF OPERATIONAL ASSESSMENT OF SECURITY OF INFORMATION AND TELECOMMUNICATION RESOURCES OF CRITICAL INFRASTRUCTURE
Kotenko Igor, Saenko Igor, Parashchuk Igor 88

AUTOMATION OF THE PROCESS OF PREPARATION OF MATERIALS WITHIN THE FRAMEWORK OF THE PUSHKIN DIGITAL PROJECT
Kotov Alexander, Kokorin Pavel ... 90

AUTHENTICATION METHODS AND THEIR ROLE IN INFORMATION PROTECTION
Krestyashin Nikita, Puchkov Vladimir ... 91

OVERVIEW OF DIGITAL SIGNATURE ALGORITHMS WITH A HIDDEN GROUP
Kurysheva Alena ... 92

CONSTRUCTION OF ATTACK FEATURES FOR A SELF-ORGANIZING DECENTRALIZED WIRELESS SENSOR NETWORK
Meleshko Aleksei ... 94

APPROACH TO THE ROLE-BASED MANAGEMENT OF WIRELESS SENSOR NETWORKS
Meleshko Aleksei ... 95

DETECTION OF ABNORMAL BEHAVIOR OF USERS AND ENTITIES IN CONTAINER SYSTEMS BASED ON MACHINE LEARNING METHODS
Melnik Maksim, Kotenko Igor ... 97

BUILDING A SPAM FILTER USING AN ARTIFICIAL NEURAL NETWORK
Mokretsov Nikita ... 99

A METHOD FOR DETECTING ANOMALOUS ACTIVITY AND VIOLATIONS OF SECURITY CRITERIA AND POLICIES IN REAL TIME
Novikova Evngenia, Kuznetsov Mikhail ... 101

CONSISTENCY SECURITY OF BIG DATA MANAGEMENT SYSTEMS
Poltavtseva Maria, Kalinin Maxim, Zegzhda Dmitry ... 102

DIGITAL FORENSICS DATA GATHERING FOR THREAT HUNTING PURPOSE
Popkov Ilya, Kotenko Igor ... 104

SYSTEMATIZATION AND GENERALIZATION OF SECURITY EVENTS
Puchkov Vladimir, Puchkov Vladimir ... 105

REDUCING THE VULNERABILITY OF PROGRAMMING TOOLS IN VARIOUS SYSTEM ENVIRONMENTS OF INFORMATION SYSTEMS
Sonichev Aleksandr, Zorin Kirill. Shchigoleva Marina, Vinogradov Aleksey ... 106

BLOCK ENCRYPTION WITH A RANDOM NUMBER GENERATOR AS A BASIS FOR DENIABLE ENCRYPTION
Tatchina Iana, Uvarov Kirill A. ... 107

DESIGNING CYBER PHYSICAL TESTBED TO ANALYSE CYBER SECURITY
Fedorchenko Elena, Novikova Evgenia, Danilov Alexandr ... 109

INVESTIGATION OF COMPUTER INCIDENTS AS A BASIS FOR OPERATIONAL ANALYSIS OF CYBERSECURITY AND A SOURCE OF SOURCE DATA FOR ARCHITECTURAL COMPONENTS OF INFORMATION SECURITY RISK MANAGEMENT
Fedorchenko Elena, Chechulin Andrey, Parashchuk Igor ... 110

APPLICATION OF A DYNAMIC FOUR-STAGE DATA PROTECTION MODEL BASED ON CRYPTOGRAPHY AND SHORTHAND IN CLOUD COMPUTING
Khlebokazov Vitaly, Kushnir Dmitry ... 112

APPROACH TO FORMING THE FEATURESOF A TARGET CYBER ATTACK FOR ATRIBUTION OF THE CYBER INTERRUPTER
Khmyrov Semyon, Kotenko Igor ... 113

INFORMATION SECURITY OF TELECOMMUNICATION NETWORKS 115

ANALYSIS OF THE PROBLEM OF DATA PROCESSING
BY UNMANNED AERIAL VEHICLES BASED ON MACHINE LEARNING METHODS
Avramenko Vladimir, Chichkov Evgeny 115

VULNERABILITIES OF SOFTWARE-DEFINED NETWORKS
Aparina Elena, Ascheulov Sergey, Babich Boris, Maier Sofia 117

PROTECTION OF NETWORK DEVICES FROM UNAUTHORIZED ACCESS
Aparina Elena, Babich Boris, Ascheulov Sergey, PatovGrigory 119

DATA PROCESSING CENTERS IN AUTOMATED INFORMATION PROCESSING SYSTEM
Asheulov Sergey, Mihaylichenko Nikolay, Gribkov Vladimir, Mishutin Nikita 123

SIMULATION MODEL OF MULTI-CHANNEL DATA TRANSMISSION MEDIUM
Verzun Natalia, Kolbanev Mikhail, Romanova Anna 125

MONITORING OF INFORMATION AND PSYCHOLOGICAL SECURITY OF THE USER BASED
ON THE INTERNET OF THINGS TECHNOLOGY
Vorobev Andrey, Andreeva Ekaterina 126

IMPLEMENTATION OF SOLUTIONS, ENSURING THE SECURITY
OF INFORMATION RESOURCES BASED ON VIRTUAL NETWORKS
Gorbunov Konstantin, Pantyukhin Oleg, Solodukhin Boris 127

ON THE ISSUE OF NETWORK SECURITY
Ilina Olga, Kupchinenko Olga, Skoropad Aleksandr 129

MANAGEMENT OF SOFTWARE PACKAGES
IN A MODERN OPERATING SYSTEM OF SPECIAL PURPOSE
Ilina Olga, Kupchinenko Olga, Skoropad Aleksandr 131

ROUTING MANAGEMENT METHODOLOGY IN DATA TRANSMISSION NETWORK
FOR UNMANNED AERIAL VEHICLE GROUPS
Kichko Yana, Sapunova Lidiya 133

CONTENT QUALITY AND SAFETY INDICFTORS
ELECTRONIC EDUCATIONAL RESOURCES
FOR THE INTEREST OF TRAINING ENGINEERING SPECIALISTS
Kryukova Elena, Parashchuk Igor 135

ABOUT USER RIGHTS IN THE OPERATING SYSTEM
Kupchinenko Olga, Ilina Olga, SkoropadAleksandr 137

IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT
OF THE DATA NETWORK BASED ON THE PREDICTION OF THE ACTIONS OF AN INTRUDER
Lipatnikov Valery, Shevchenko Alexander, Melekhov Kirill 139

ANALYSIS OF THE CAUSES OF DISTORTION
OF THE DIRECTIONAL PATTERNS BROADBAND ANTENNAS
Lyanguzov Danila 141

USING MIKROTIK ROUTERS WHEN BUILDING SECURE DATA TRANSMISSION NETWORKS
Mandrick Dmitry, Sazonov Viktor 142

CRITERIA FOR SELECTING THE ENERGY SAVING ROUTE
TRANSMISSIONS FOR HIGH DENSITY WIRELESS SENSOR NETWORKS
Maslova Daria 143

ANALYSIS OF WAYS TO CREATE ABSORBING BOUNDARY CONDITIONS
IN THE FINITE DIFFERENCE METHOD IN THE TIME DOMAIN
Meshalkin Valentin, Shanin Alexander, Konkov Denis, Tkachev Dmitry 144

ROUTING METHODS FOR PED-UP WIRELESS SENSOR NETWORKS
Miklush Vuktoria 145

INFORMATION SECURITY AND TECHNICAL RELIABILITY OF MOBILE DATA CENTERS:
AN APPROACH TO THE FORMATION OF INDICATORS FOR CURRENT AND PROACTIVE CONTROL
Mikhailichenko Anton, Parashchuk Igor, Seleznev Andrey 146

ANALYSIS OF APPLICATION OF ELEMENTS OF ARTIFICIAL INTELLIGENCE
IN THE EDUCATIONAL ACTIVITY OF A TECHNICAL UNIVERSITY
Mnatsakanyan Vladislav, Novoselov Sergey, Pantyukhin Oleg 148

APPROACH TO BUILDING A COMPLEX TECHNICAL SYSTEM MODEL
Ostroumov Oleg, Leptchkin Oleg, Sinyk Aleksander, RenskovDmitrii 150

FUNCTIONING PROFILE OF A COMPLEX TECHNICAL SYSTEM
Perov Roman, Ostroumov Oleg, Filimonov Vasily 151

ON THE ISSUE OF USING DYNAMIC ROUTING PROTOCOLS
IN SPECIAL PURPOSE DATA TRANSMISSION NETWORKS
Marina Rubtsova, Viktor Sazonov 153

MACHINE LEARNING-BASED ANOMALIE DETECTION METHOD IN SQL QUERIES
Ryumina Svetlana, Saenko Igor 154

UNMANNED AERIAL VEHICLES AND SECURITY DATA CENTERS
Ryazanceva Polina, Mihaylichenko Nikolay, Gribkov Vladimir, Asheulov Sergey 156

ASPECTS OF ENSURING INFORMATION SECURITY OF DOCUMENT MANAGEMENT AUTOMATION
SYSTEMS, TAKING INTO ACCOUNT THE RISK ANALYSIS OF THEIR SECURITY
Sayarkin Vitaly, Parashchuk Igor 158

THE DEVELOPMENT OF QUANTUM TECHNOLOGIES AND THEIR IMPACT
ON THE INFORMATION SECURITY OF DATA CENTERS
Sergeev Valeriy, Mihaylichenko Nikolay, Gribkov Vladimir, Mishutin Nikita 160

USE OF THE TOOLS FOR BACKUP AND RECOVERY OF INFORMATION IN DATABASES
Skoropad Aleksandr, Ilina Olga, Kupchinenko Olga 162

BUILDING A COMPUTER SUPPORT SYSTEM SPECIAL EXERCISES (GAMES)
Solodukhin Boris, Pantyukhin Oleg, Kovalev Igor, Pashchenko Vasily, Ryabov Gennady 164

PREDICTIVE CONTROL OF THE FUNCTIONAL STABILITY OF A COMPLEX TECHNICAL SYSTEM
Sergey Teslya, Oleg Ostroumov, Semyon Shinkarev 166

ANALYSIS OF WAYS TO REDUCE THE IMPACT OF CHANNEL AND PATH CONGESTION
ON THE PERFORMANCE OF A SPECIALIZED DATA TRANSMISSION NETWORK
DURING ITS OPERATION
TitovVladimr, Aparina Elena, Babich Boris, Ascheulov Sergey 168

APPLICATION OF GENERATIVE ADVERSARIAL NETWORKS
FOR DATABASE SYNCHRONIZATION IN SPECIAL-PURPOSE INFORMATION SYSTEMS
Udal’tsov Alexander, Saenko Igor 170

APPROACH TO DETECTION AND AUTOMATIC CLASSIFICATION
OF UNAUTHORIZED IMPACTS ON INFORMATION TELECOMMUNICATION SYSTEM
Usov Nikolay, Philimonov Vasiliy, Ostroumov Oleg 171

GENERAL APPROACH TO SIGNALS DEMODULATION WITH DIGITAL PHASE MODULATION
IN THE HIGH FREQUENCY COMMUNICATION SYSTEMS
Usov Nikolay, Philimonov Vasiliy, Ostroumov Oleg 173

INCREASING THE SECURITY OF A SENSOR NETWORK
BY USING A DISTRIBUTED VIRTUAL MACHINE
Shalnev Ilia 174

TASKS OF SYNTHESIS OF THE TOPOLOGICAL STRUCTURE OF THE DATA TRANSMISSION NETWORK TAKING INTO ACCOUNT THE PARAMETERS OF INFORMATION SECURITY
Shinkarev Semyon, Parashchuk Igor 175

APPLICATION OF THE METHOD OF EXTREME ORDER STATISTICS FOR ESTIMATION OF SMALL PROBABILITIES OF RANDOM VARIABLES
Yankovskii Nikita 177

THE INTERCONNECTION OF MACHINE VISION AND INFORMATION SECURITY
Yarovoy Robert, Parashchuk Igor 178

INFORMATION AND ECONOMIC SECURITY 181

APPROACHES TO ENSURING INFORMATION SECURITY IN THE ACTIVITIES OF THE GAME DEVELOPMENT COMPANIES
Aminov Khakimdzhon, Urvantsev Roman 181

RUSSIAN AND FOREIGN EXPERIENCE OF DIGITALIZATION WATER SUPPLY AND SANITATION SYSTEMS
Anikin Yuri, Shilkov Vladimir, Ushakova Ludmila 183

IMPROVING SECURITY METHODS IN RADIO FREQUENCY AUTHORIZATION SYSTEMS
Emelyanov Alexandr, Melikhova Valentina 185

PRIORITY MODEL OF THE DATA EXCHANGE PROCESS IN A DIGITAL DOUBLE
Krasnova Anna, Kolbanev Mikhail 186

DIGITAL AGRICULTURE: NEW TECHNOLOGIES TO IMPROVE EFFICIENCY AND SAFETY IN AGRICULTURE
Maslov Nikita 187

THE ROLE OF THE INTERNAL TIME ASYMMETRY PHENOMENON IN THE DURABILITY THEORY OF COMPLEX DYNAMIC SYSTEMS
Ostreikovskii Vladislav, Sorochkin Andrei 189

APPLICATION OF SIMULATION MODELING FOR SOLVING PROBLEMS OF NETWORK PLANNING
Puha Gennady 191

MATHEMATICAL MODEL OF CONFIDENTIAL INFORMATION SAFETY-CONSCIOUS ENTERPRISE MANAGEMENT
Sokolov Roman 192

ANALOGIES OF DATA REPRESENTATIONS. COMPARISON OF VERBAL QUANTITIES: ECONOMY, PLANNED ECONOMY, MARKET ECONOMY
Yaroshevich Ludmila 193

INFORMATION SECURITY OF TRANSPORT SYSTEMS 194

APPLICATION OF ERP- AND MES-SYSTEMS IN THE SHIPBUILDING INDUSTRY
Antonova Alena, Sokolov Sergey 194

SIMULATION OF SAFE TRANSPORT CONTROL SYSTEMS
Goloskokov Konstantin, Astapkovich Alexey, Korotkrv Vitaly 195

DETERMINATION OF THE MOTION INDICATORS OF AN AUTONOMOUS VESSEL USING THE MAPLE 12 SOFTWARE PACKAGE
Danilin German, Sokolov Sergey 196

SAFE SYSTEM FOR OIL SPILL MONITORING USING UNMANNED AERIAL VEHICLES
Egorova Kristina, Sokolov Sergey 197

MODELS OF INFORMATION PROCESSING
Zubanova Anastasia, Kogtev Alexey 198

CREATION OF SECURE INFORMATION SYSTEMS FOR TRANSPORT LOGISTICS BASED ON MULTI-AGENT APPROACH
Iskanderov Yury 199

INFORMATION SECURITY SUBSYSTEM FOR INTELLIGENT SUPPORT FOR TRANSPORTATION OF OVERSIZED CARGO
Iskanderov Yury, Chumak Alexandr, Shakhnov Sergey 201

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN THE DEVELOPMENT OF ALGORITHMIC SUPPORT FOR FORECASTING OF AUTOMATED CONTROL SYSTEMS
Kapustin Artem 202

PROVIDING SAFE FUNCTIONING OF TRANSPORT SYSTEMS
Klionskiy Dmitry 204

POSSIBILITIES OF USING ARTIFICIAL INTELLIGENCE TECHNOLOGY IN WATER TRANSPORT
Kotov Aleksandr 205

A MECHANISM FOR PROVIDING COMPLETE RANDOMIZATION OF A DIGITAL SIGNATURE IN ALGEBRAIC ALGORITHMS WITH A HIDDEN GROUP
Moldovyan Alexandr, Morozova Elena 206

APPLICATION OF VECTOR FINITE FIELDS IN DEVELOPMENT OF THE MULTIVARIATE CRYPTOGRAPHY ALGORITHMS
Morozova Elena, Moldovyan Nikolay, Kostina Anna 208

ON THE APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS IN SYSTEMS FOR PROTECTING TRANSPORT NETWORKS FROM CYBER ATTACKS
Nyrkov Andrey, Bogdanova Polina, Prokopenko Daniil 210

INTRUSION DETECTION METHODS IN COMPUTER NETWORKS OF TRANSPORT INDUSTRY
Nyrkov Anatoliy, Yumasheva Elena, Nyrkov Andrey 212

SOFTWARE COMPLEX FOR GENERATING SECURE PASSWORDS
Skobelev Alexey, Goloskokov Konstantin 214

DIALOGUE MODULES «AIS IT CLINIC»
Shipunov Ilya, Nyrkov Anatoliy, Rotnov Dmitry, Shipunova Diana 215

ON THE SECURITY OF THE COMMUNICATION MODULES «AIS IT CLINIC»
Shipunov Ilya, Nyrkov Anatoliy, Shipunova Diana 216

INFORMATION SECURITY OF MARINE EQUIPMENT OBJECTS AND MARINE INFRASTRUCTURE 218

IS-ASPECT OF INFORMATION SEARCH ENGINES
Azikova Anna, Ozerova Ksenia, Danilchik Andrey 218

METHODOLOGY OF CREATION AND EDUCATIONAL AND LABORATORY USE DIGITAL COUNTERPARTS OF SHIP AUTOMATION SYSTEMS AND AUDIT OF THEIR INFORMATION SECURITY
Alekseev Anatoly, Sogonov Sergey, Maximova Marina,
Khrutsky Oleg, Ravin Alexander, Mikhalchuk Andrey 220

DIGITALIZATION OF SELF-CONTROL OF THE DEVELOPMENT INFORMATION WARFARE TECHNOLOGIES IN ADVANCED TRAINING
Alekseev Anatoly, Mikhalchuk Andrey, Musatenko Roman 222

INFORMATION SURVIVABILITY OF MANAGEMENT:
THEORY AND PRACTICE OF ENSURING INFORMATION SUPERIORITY
Alekseev Anatoly Vladimirovich 224

DIGITAL TWIN OF PROCESS AUTOMATION SYSTEMS FOR FIGHTING FOR INFORMATION SURVIVABILITY OF SHIP, PRODUCTION SAFETY MONITORING
Alekseev Anatoly, Antipov Vasily, Smolnikov Alexander 226

CONTROL OVER THE MANIFESTATION OF A DEPRESSIVE STATE AMONG SPECIALISTS OF THE MARINE AND RIVER FLEET, AS A DIRECTION FOR IMPROVING THE SAFETY OF NAVIGATION
Artemov Stanislav, Alekseev Sergey, Ryabkov Yakov 228

COMPARATIVE ANALYSIS OF INFORMATION VITALITY «EAM» CLASS SOFTWARE SYSTEMS
Bondarenko Andrey, Goloviznina Olga, Alekseev Anatoly 230

ASSESSMENT OF THE USE OF MRP CLASS INFORMATION TECHNOLOGIES IN THE LIFE CYCLE OF A MARINE EQUIPMENT OBJECT AND THEIR APPLICATION
Goloviznina Olga, Rodomanova Kristina, Alekseev Anatoly 232

QUALIMETRIC RANKING OF INFORMATION TECHNOLOGIES OF THE «WMS» CLASS IN ROTECTED EXECUTION AND THEIR PRACTICAL DEVELOPMENT
Goloviznina Olga, Rodomanova Kristina, Bondarenko Andrey, Alekseev Anatoly 233

DIGITAL TWIN OF SOFTWARE IMPLEMENTATION TOOLS
CRM SERVICE IN PROTECTED EXECUTION
Egorov Ahmed, Durkin Ilya, Nikonorov Vladislav, Edoshin Alexander 235

QUALIMETRIC RANKING OF INFORMATION TECHNOLOGIES OF THE CLASS «PDM»
IN THE HOUSING AND COMMUNAL SERVICES OF THE TYPE OF JSC CMKB «ALMAZ»
AND THEIR PRACTICAL DEVELOPMENT
Parastaeva Elena, Kalinina Elena, Tyurina Natalia, Alekseev Anatoly 238

THE TASK OF FINDING THE OPTIMAL POSITION OF THE CONTROL CENTER IN A SAFE EXECUTION IN A HIGH-RISE BUILDING OF THE MARINE INFRASTRUCTURE
Plotnikov Pavel, Alekseev Sergey 240

PRINCIPLES OF AUTOMATION OF MANAGEMENT IN THE PROTECTED EXECUTION
OF SCIENTIFIC AND INDUSTRIAL ASSOCIATIONS OF MARINE INFRASTRUCTURE
Ryabkov Yakov, Alekseev Sergey, Artemov Stanislav 241

FORMATION OF A LIST OF RECOMMENDATIONS FOR MODERNIZING THE INFORMATION SECURITY SYSTEM BASED ON THE RESULTS OF ASSESSING THE ENTERPRISE MATURITY LEVEL
Tarasov Valentin, Kudinova Ekaterina 243

RANKING OF INFORMATION TECHNOLOGIES CLASS «FM» IN A PROTECTED VERSION
Yurkov Anton 245

INFORMATION AND PSYCHOLOGICAL SECURITY 247

SIGNIFICATIVE DENOTATIVE TRANSFER TO MIND MANIPULATION TECHNOLOGY
Belomestnova Nina 247

METHODS OF COUNTERING INFORMATION AND POLITICAL IMPACT ON AN OFFICIAL
Borshenko Viktor 248

SOCIOCULTURAL TRANSFORMATION OF UKRAINIAN SOCIETY: ALTERNATIVE CONCEPTS IN THE CONTEXT OF EVOLUTIONARY AND CYCLICAL THEORIES
Degtyareva Olga 251

COGNITIVE SECURITY TECHNOLOGIES ON THE WAY OF INTEGRATION
Kefeli Igor 253

LEGAL BASIS FOR COGNITIVE SECURITY
Kirilenko Viktor Petrovich, Alekseev Georgy Valerievich 255

MEDIA IMAGE OF MODERN RUSSIA IN GREEK MASS MEDIA
Kuchinskaya Yana 256

ARTIFICIAL INTELLIGENCE IN THE MEDIA SPHERE:
PROGRESS OR A THREAT TO INFORMATION SECURITY?
Lai Lingzhi 257

INFLUENCE OF NETWORK MEDIA ON PHOBIAS AND THE LEVEL OF PSYCHOLOGICAL ANXIETY IN THE ASPECT OF COGNITIVE SECURITY
Melnik Veronica 259

MEDIA RESOURCES IN INFORMATION AND PSYCHOLOGICAL ATTACKS ON RUSSIAN STATEHOOD
Melnik Galina 260

GERMAN MASS MEDIA AS A MEANS OF COGNITIVE DISTORTION OF REALITY
Misonzhnikov Boris 262

ON THE QUESTION OF THE CONCEPT OF COGNITIVE SPACE
Plebanek Olga 264

RAMING THEORY AND POLITICIZATION OF THE MEDIA (ON THE EXAMPLE OF WESTERN MEDIA SILENCING THE PROBLEM OF JAPAN DUMPING NUCLEAR WASTE INTO THE SEA)
Tan Leyi 266

MEDIA CONSUMPTION: PROCESSES, CHARACTERISTICS, TRENDS
Tiunina Ekaterina 268

ANALYSIS OF BEHAVIOR AND PSYCHOLOGY OF VERBAL VIOLENCE AMONG INTERNET MEDIA USERS
Zhou Shengnan 270

NEUROSCIENCE IS THE BASIS FOR THE STUDY OF BRAIN FEATURES AND MODELING OF VARIOUS COGNITIVE–BEHAVIORAL PROCESSES
Shangin Anlrey 271

MAIN DIRECTIONS OF INFORMATION AND DISRUPTIVE ACTIVITIES OF THE WEST AGAINST THE RUSSIAN FEDERATION: POLITICAL ANALYSIS
Shevtsov Vladimir 273

INFORMATION SECURITY IN SOCIOCOMPUTTING 276

A WAY TO SPEED UP GLOBAL POSTERIOR INFERENCE USING TERTIARY STRUCTURE
Abramov Maxim, Vyatkin Artyom 276

SOCIO-PSYCHOLOGICAL FACTORS OF ENSURING THE SECURITY AND FUNCTIONING OF STATE INFORMATION SYSTEMS IN THE CONTEXT OF SOCIO-ENGINEERING ATTACKS
Artur Azarov, Mikhail Demidov, Pavel Savelev 278

DIGITAL SLAVERY AS A THREAT TO DIGITAL TRANSFER INDIVIDUALS, SOCIETIES, STATES
Alekseev Anatoly 279

PROTECT AGAINST PHISHING ATTACKS
Bobryshov Danil, Zacepin Ilya, Chuvaev Konstantin 281

THE TASK OF DEVELOPING A SERVICE FOR PLANNING THE COST OF A VEHICLE ROUTE TAKEN INTO ACCOUNT OF USER PARAMETERS
Korepanova Anastasia, Esin Maksim, Sabrekov Artem 282

LOGISTICS PORTAL CARGOTIME.RU: AUTOMATION OF MONITORING THE STABILITY OF THE DELIVERY COST CALCULATION SERVICE
Nazarova Polina, Esin Maxim, Sabrekov Artem 284

DEVELOPMENT OF A METHOD FOR DETECTING FAKE ACCOUNTS IN SOCIAL NETWORKS
Nizomutdinov Boris 287

APPLICATION OF LOGIC-EVENT MODELING TO DESCRIBE CRITICAL PHASES OF DEVELOPMENT OF SOCIO-INFORMATION PROCESSES
Perevaryukha Andrey, Manvelova Aleksandra, Trofimova Inna, Mikhailov Vladimir, Hasanov Dmitry 289

INFORMATION SECURITY OF CYBERPHYSICAL SYSTEMS 291

APPLICATION OF METHODS OF COMPUTER MATHEMATICS AND MULTISCALE ANALYSIS TO DETECT INTRUSIONS INTO INFORMATION SYSTEMS
Bortniker Peter, Saenko Igor 291

DESCRIPTION OF PATTERN RECOGNITION TECHNOLOGY FOR DETECTING ROAD ACCIDENTS
Galeeva Evgenia 292

RECOGNIZING ACCIDENTS USING COMPUTER VISION
Golovkin Matvey 293

METHOD SYMBIOTIC OF INTERACTION OF NEURAL NETWORKS WITH NO ANTAGONISTIC GAME ELEMENTS IN PROBLEMS OF ENSURING THE SECURITY OF DATA SETS
Gololobov Nikita, Pavlenko Evgeniy 294

METHOD FOR BUILDING A MEASURING NETWORK FOR ELECTROMAGNETIC RADIATION ON IoT CONTROLLERS
Kuleshov Sergey, Aksenov Alexey 296

THE COMBINATION OF THE CONCEPTS OF OPENNESS AND SECURITY IN THE PROTOTYPE OF A DISTRIBUTED SYSTEM
Nechitailenko Roman, Glushchenko Artem, Denisov Egor 297

METHODS OF ENSURING INFORMATION SECURITY OF WIRELESS SELF-ORGANIZING NETWORKS
Pahomov Maksim, Sobolev Nikolay, Pavlenko Evgeny 299

DATA CLUSTERIZATION USING KOHONEN NEURAL NETWORK
Shvayko Aleksander 301

PRINCIPLES OF BUILDING A SELF-ORGANIZING NEURAL NETWORK MAP FOR THE ARCHITECTURE OF A SECURE INTELLIGENT INTRUSION AND INCIDENT DETECTION SYSTEM
Shterenberg Stanislav 302

APPLICATION OF MACHINE VISION TECHNOLOGY IN LIMITED RESOURCE CONDITIONS
Yakovleva Ekaterina 303

ONE OF THE WAYS TO ENSURE THE SECURITY OF AN EDUCATIONAL INSTITUTION ON A SINGLE PLATFORM
Yankovskii Nikita, Tatarnikova Tatiana 305

TRAINING AND RETRAINING OF PERSONNEL IN THE FIELD OF SECURITY INFORMATION SECURITY 307

IMPROVEMENT OF PEDAGOGICAL METHODS THROUGH THE USE OF VIRTUAL LABORATORY PRACTICE WHEN STUDYING THE BASICS OF CRYPTOGRAPHIC INFORMATION PROTECTION BY CADETS
Voronov Sergey, Primakin Alexey 307

TRAINING FOR FUTURE MANAGEMENT STAFF UNMANNED AERIAL VEHICLES
Grachev Alexander 308

FIGHTING THREATS IN SOCIAL NETWORKS
Kononov Oleg, Kononova Olga 309

AUTOMATED CONTROL SYSTEM FOR THE PROCESS OF CONDUCTING STUDENTS CLINICAL PRACTICE IN PROTECTED VERSION
Safronova Marya, Nyrkov Anatoliy 311

DEVELOPMENT OF A DIGITAL EXCHANGE OF RESEARCH RESULTS
Solomatova Maria, Smelov Ilya, Dotsaev Timur, Pak Vladislav 313

STUDYING THE MECHANISMS OF ISOLATION OF OPERATING SYSTEM RESOURCES DURING THE TRAINING OF SPECIALISTS IN «COMPUTER SECURITY»
Chastuhin Daniil, Shirokov Vladimir, Schigoleva Marina 314

VIRTUAL SIMULATOR AS A WAY OF TRAINING FUTURE SPECIALISTS IN TECHNICAL PROTECTION OF INFORMATION
Sheikhov Gleb, Lipatnikov Valery, Ostrovsky Yuri, Vasiliev Nikita, Ledovskaya Kristina 316

THE PROJECT «IT CLINICS» IN ADMIRAL MAKAROV SUMIS
Shipunov Ilya, Nyrkov Anatoliy, Shipunova Diana 317

YOUTH SCIENTIFIC SCHOOL «ECOSYSTEM OF SAFE CITY DIGITAL SERVICES» 320

DIGITAL SERVICES EVALUATION FRAMEWORKS: A REVIEW
Arkatov Dmitriy 320

PENETRATION OF DIGITAL MEDICAL SERVICES INTO THE ENVIRONMENT OF ELDERLY RESIDENTS OF PETERSBURG
Vidiasova Lyudmila, Tolstikova Irina 321

THE USE OF DIGITAL PUBLIC SERVICES AS A FACTOR OF SOCIAL WELL-BEING: THE EXAMPLE OF ST. PETERSBURG
Vidiasova Lyudmila, Yakubova Maria 322

THE RIGHT TO REFUSE DIGITAL TECHNOLOGIES IN THE CONTEXT OF DYNAMIC DIGITIZATION OF SOCIETY
Denisov Denis 324

DEVELOPMENT OF DIGITAL HEALTH SERVICES TO OPTIMIZE CITY BUDGET COSTS FOR FINANCING PHARMACOTHERAPY FOR PATIENTS WITH ONCOLOGICAL DISEASES
Kanevsky Maxim 326

PERCEPTION OF DIGITAL PUBLIC SERVICES BY CIVIL ACTIVISTS OF ST. PETERSBURG
Kiseleva Darya, Sungurov Alexander 327

ANALYSIS OF THE IMPLEMENTATION OF THE ECOSYSTEM OF CITY SERVICES «DIGITAL PETERSBURG»
Kuznetsov Aleksei 329

THE USE OF DIGITAL SERVICES IN THE MUNICIPALITIES OF ST. PETERSBURG
Meteleva Alina, Slav Julia, Filatova Olga 330

ECOSYSTEM OF CITY SERVICES «DIGITAL PETERSBURG»
Osmolovsky Kirill 332

ENSURING THE SECURITY OF DIGITAL SERVICES WITH CONSIDERATION FOR THE TRUST SPECIFICS OF ELDERLY USERS TOWARDS ONLINE PLATFORMS
Ravchik Mihail 333

DEVELOPMENT OF A DATABASE OF DESTRUCTIVE CONTENT BASED ON DATA FROM MESSENGERS
Uglova Anna, Nizomutdinov Boris 335

ROLE MODEL OF THE URBAN SERVICE ECOSYSTEM: BUSINESS NEEDS RESEARCH
Yuplanov Mark 336

YOUTH SCIENTIFIC SCHOOL «SAFE INTELLIGENT INFORMATION SYSTEMS AND TECHNOLOGIES» 339

USAGE OF NEURAL NETWORKS IN THE SOLUTION OF AUTONOMOUS NAVIGATION OF UNMANNED AERIAL VEHICLES
Belyaev Pavel, Zikratov Igor 339

CURRENT STATE AND PROSPECTS FOR THE DEVELOPMENT OF DIGITAL TWINS OF SPATIAL OBJECTS
Verhova Galina, Akimov Sergei, Proshchenkov Valerii, Iurchik Daniil 340

RESEARCH AND DEVELOPMENT OF DYNAMIC STEGANOGRAPHY ALGORITHMS FOR GRAPHIC CONTAINERS
Volynkin Pavel, Gibadullin Albert 341

DEVELOPMENT OF METHODS, ALGORITHMIC AND SOFTWARE FOR ASSESSING THE QUALITY OF ENCRYPTION CONTAINERS
Volynkin Pavel, Kuznetsov Vadim 342

SPECIFICITY OF ANALYSIS OF WLAN TRAFFIC WITH WPA2-ENTERPRISE STANDART
Gerling Ekaterina, Zebzeev Egor, Kistruga Anton 343

RESEARCH ON INFORMATION MODEL FOR ASSESSING STUDENT LEARNING LEVELS IN TESTING
Gubin Alexander, Mikhaylova Ekaterina 344

ATTACK DETECTION ON TDLS WIRELESS DEVICE
Drepa Vladislav, Kovtsur Maxim, Sakharov Dmitry, Sharapov Roman 345

INVESTIGATION OF NEW APPROACH TO INVESTIGATING THE INTEGRITY OF THE LINUX OPERATING SYSTEM DURING ITS OPERATION
Konkov Vladimir, Kuznetsov Vladimir, Krasov Andrey 346

COMPARATIVE ANALYSIS OF LIBRARIES FOR NATURAL LANGUAGE PROCESSING TASKS
Kopytova Elena, Philippov Felix 348

CHOOSING A LINUX KERNEL MODULE FOR IMPLEMENTING A DIGITAL WATERMARK
Krasov Andrey 350

THREATS TO INFORMATION SECURITY IN NEURAL NETWORK TECHNOLOGIES
Litvinov Vladislav, Balakirev Nikolai 351

PRINCIPLES OF SAFE DESIGN OF INFORMATION SYSTEMS
Litvinov Vladislav, Bezkorovayinya Maria, Tolmachev Andrey, Goldes Ilya 353

RESEARCH OF SIMULATION MODELING METHODS THE PROCESSES OF THE SPREAD OF THE EPIDEMIC
Litvinov Vladislav, Dergachev Daniil 354

DEVELOPMENT OF MEANS TO PROTECT INFORMATION SYSTEMS FROM THE MALICIOUS USE OF ARTIFICIAL INTELLIGENCE
Litvinov Vladislav, Goldes Ilya, Bezkorovayinya Maria, Tolmachev Andrey 355

ANALYSIS OF ATTACKS ON THE NETWORK NODES OF GROUP ROBOTS
Litvinov Vladislav, Yashin Alexey 356

METHOD OF FORMATION OF MANAGEMENT DECISIONSIN SPECIAL PURPOSE TELECOMMUNICATION NETWORKSTAKING INTO ACCOUNT THE AVAILABLE RESOURCES
Lipatnikov Valery, Parfirov Vitaly, Petrenko Mikhail 358

RESEARCH OF METHODS FOR EVALUATING AND IMPROVING THE PERFORMANCE OF A WIRELESS NETWORK
Makhmutova Nuriia, Kovzur Maxim, Petrova Tatiana, Kistruga Anton 359

STUDY OF SOFTWARE STRUCTURE OF LTE RADIO ACCESS NETWORK ARCHITECTURE
Moshak Nikolay, Kravets Alexey 360

IPX NEW PARADIGM FOR CONVERGENCE OF NGN MOBILE AND FIXED NETWORKS
Moshak Nikolay, Medvedev Dmitry 363

ANALYSIS OF DISTRIBUTED ACTION PLANNING IN MULTI-AGENT SYSTEMS
Pelikh Dmitry, Ptitsyna Larisa, Shirin Alexander 364

THE WEBSPLOIT TOOLKIT FOR WIRELESS NETWORK
INFORMATION SECURITY ASSESSMENT
Petrova Tatyana, Kuzmina Olga, Kovzur Maxim, Kistruga Anton 365

ONTOLOGY OF ARCHITECTURE OF INTELLIGENT INFORMATION SYSTEMS
FOR FORECASTING STOCK QUOTES
Ptitsyn Nikita, Ptitsyna Larisa 367

MICROSERVICES TO IMPROVE THE QUALITY OF INFORMATION SEARCH
Ptitsyna Larisa, Soltyk Alexey 368

INTRUSION DETECTION BASED ON IMMUNOCOMPUTING
Tyumentsev Aleksey, Bondarenko Igor 369

APPLICATION OF THE THEORY OF BIFURCATIONS FOR THE ANALYSIS OF CYBER SECURITY OF
OBJECTS OF CRITICAL INFRASTRUCTURE
Shashkin Vladislav, Petrova Tatiana, Birikh Ernest, Sakharov Dmitrii, Lipatnikov Valery 371